ELECTRONIC DISCOVERY

Not Just for Mega-Clients: Why You and Your Smaller Clients Need to be Concerned with Electronically Stored Information

By Rex B. Stratton

JUNE 2005

STRATTON BALLEW PLLC
18850 – 103rd Ave, SW, Suite 102
Vashon Island, WA 98070
206.682-1496
stratton@strattonballew.com

REX B. STRATTON has over thirty years of experience representing U.S. and foreign clients in business law and management, litigation, corporate finance and secured transactions, as well as an extensive background in both litigation and transactional matters involving patent, trademark, copyright and trade secrets. He was Law Clerk to the Honorable William J. Jameson (D. Mont.); he is past president of the Washington State Patent Law Association; member of the Board of Directors of the American Intellectual Property Law Association (2000 - 2003); a member of the AIPLA Fellows and a Trustee of the American Intellectual Property Law Education Foundation (2000 to date).

One Fish - Two Fish -- Big Fish - ***Little Fish***
These rules apply to you

A. E-Discovery is Not Just for the Big Guys

Zubulake v. UBS Warburg LLC did not limit its holding to only the Big Fish. From the perspective of a small law firm or solo attorney, two of the Zubulake cost shifting cases are worth noting carefully. These two cases are good guidelines for discovery compliance in the context of what e-data is and how it is retained.

- *Zubulake v. UBS Warburg LLC*, 217 F.R.D. 309 (S.D.N.Y. 2003) ("Zubulake I") sets forth a seven-factor test for determining whether to shift the cost of discovery. (1) is request is tailored to discover relevant information; (2) is the information from other sources; (3) the production costs compared to the amount in controversy; (4) the total cost of production compared to the resources available to each party; (5) the relative ability of each party to control costs and its incentive to do so; (6) the importance of the issues at stake in the litigation; and (7) the relative benefits to the parties of obtaining the information. The first two factors are entitled to the greatest weight. Zubulake court concludes that cost-shifting should be considered only when electronic data is relatively inaccessible.

- *Zubulake v. UBS Warburg LLC*, 216 F.R.D. 280 (S.D.N.Y. 2003) ("Zubulake III") After receiving evidence of the costs and results of the initial test sample, the Court ordered restoration of the remaining back-up tapes and applying the seven-point test and ordered that plaintiff pay 25% of the cost of restoring the data and conducting word searches for the relevant names and subjects. But the Court holds that defendant's costs for attorneys to review the restored data for relevancy and privilege would not be shared.

Zubulake I (*Zubulake v. UBS Warburg LLC*, 217 F.R.D. 309 (S.D.N.Y. 2003)) manifests that if *e*-data is "accessible" it must be produced at the expense of the responding party. If *e*-data is "inaccessible" (not readily usable) then the cost shifting analysis comes in to play. However, the inherent cost of satellite motion practice to reach "inaccessible" data may, in the first instance, be prohibitive for Little Fish.[1] Too, Little Fish maybe be required to produce inaccessible *e*-data without the benefit of cost shifting if it did not preserve the *e*-data as and when it was supposed to.

[1] "Courts must remember that cost-shifting may effectively end discovery, especially when private parties are engaged in litigation with large corporations." *Zubulake I*, 217 F.R.D. at 317.

While Rule 26(b) (2) provides a ***proportionality test***, it does not exempt Little Fish from the Rules. Rule 26(c) is not a safe harbor for Little Fish that do not preserve evidence.

From the perspective of the small company or individual party, even having to share in 25% of the cost of e-discovery could be prohibitive. For Little Fish *e*-discovery is not a clever game just to be played. Little Fish are best protected by careful observance and thoughtful, well crafted discovery. If a Little Fish asks a Big Fish to produce all e-mails that refer, reflect or relate to a claim or defense, the request may cost more than the Little Fish thinks and the results may be overwhelming. The flip side is a Little Fish may be compelled to produce inaccessible *e*-data without cost shifting to the Big Fish.

B. Rules of the Road for Little Fish:

- Look to proving your case from your client's files and records to the greatest extent possible.
    - Make sure that your client retains it's records:
        - you need all the data you can mine from your client, and
        - even Little Fish plaintiffs have to respond to *e*-discovery.
- Carefully craft discovery to elicit only the information and evidence that you really need to prove your case.
    - Overly aggressive discovery can be costly to Little Fish in pursuing or defending satellite discovery practice.
    - Hardball tactics have not disappeared:
        - the more you look to the other side's files and records to prove your case, the more you expose yourself and your client to having to play hardball with the other side, and
        - the worse shape your clients *e*-data is in, the more you expose your client to hardball tactics to obtain *e*-data or assert spoliation against your client's claims or defenses.
- But, remember, *e*-data can be a wonderfully fertile area of discovery, if you know how to get at it, distill it and analyze it. Even Little Fish, with the right tools, can be successful in *e*-discovery.

Small Firm Caveat: If you are not an expert on e-data storage and recovery, find an Information Technology (IT)expert now and keep the relationship strong – you will need Information Technology assistance in the new era of *e*-discovery litigation regardless of which side your client may be on.

C. Use Rule 26(a) (1) and the Rule 26(f) Conference to Your Advantage

The Proposed rules provide that as soon as practicable after a lawsuit is filed, the parties must meet to discuss any issues relating to the preservation of electronically stored information and to develop a discovery plan concerning any issues relating to disclosure or discovery of electronically stored information, including the form or forms in which it should be produced and any issues relating to claims of privilege or protection of trial preparation materials. A report outlining how the discovery of electronically stored information should be handled must be submitted to the court within fourteen days of the meeting. The parties must then provide to the other parties a copy or description of all electronically stored information that the disclosing party may use.[2] But, why wait to get started?

In fact, do not wait until the Rule 26(f) conference to begin building your client's case for production of e-discovery. A Rule 26(f) conference letter can be effectively used to set the stage for *e*-discovery and for data you expect the other side will be disclosing under Rule 26(a)(1). (See Appendix A for an example.). A Rule 26(f) conference letter:

- Puts the other side on notice of what areas of discovery, especially e-data you are looking to have voluntarily produced.
- Permits better use of Interrogatories and requests for production of documents to focus on discovery not produced pursuant to Rule 26(a)(1).
- Permits the argument that the other side failed to meet the initial disclosure requirements of Rule 26 when seeking to drill down in obtaining relevant documents, including *e*-data.

D. Duty to Preserve – Can Little Fish Afford Big Fish Requirements

For the attorney who represents smaller clients, the observations of Judge Scheindlin in *Zubulake IV*[3] on the duty to preserve evidence need careful review. In *Zubulake V* [4] Judge Scheindlin asks this rhetorical question, which she then answers for the bar:

---

[2] Proposed FRCP 26(a)(1)(B), FRCP 26(f), FRCP 26(f)(3), FRCP 26(f)(4), FRCP 26(f)(7) and Form 35.
[3] *Zubulake v. UBS Warburg LLC*, 229 F.R.D. 212 (S.D.N.Y. 2003)
[4] *Zubulake v. UBS Warburg LLC*, 229 F.R.D. 422, 433 -34 (S.D.N.Y. 2004)

What must a lawyer do to make certain that relevant information – especially electronic information – is being retained?

***

First, counsel must issue a "litigation hold" at the outset of litigation or whenever litigation is reasonably anticipated.[5] The litigation hold should be periodically re-issued so that new employees are aware of it, and so that it is fresh in the minds of all employees.

Second, counsel should communicate directly with the "key players" in the litigation, *i.e.*, the people identified in a party's initial disclosure and any subsequent supplementation thereto. Because these "key players" are the "employees likely to have relevant information," it is particularly important that the preservation duty be communicated clearly to them. As with the litigation hold, the key players should be periodically reminded that the preservation duty is still in place.

Finally, counsel should instruct all employees to produce electronic copies of their relevant active files. Counsel must also make sure that all backup media which the party is required to retain is identified and stored in a safe place.

Little Fish may not have sophistication as to *e*-data. The lawyer who advises a Little Fish as to *e*-discovery matters take on far greater responsibility than that of the lawyer advising a Big Fish that has IT personnel and sophisticated systems.

- **Litigation Hold.** A Little Fish may not understand what it is required to do with its *e*-data to satisfy a litigation hold or even how to do it. Simply telling the client what the law requires may not suffice. Counsel for a Little Fish should not rely on the client's sophistication. Although the responsibility ultimately rests with the client, lawyers still have an obligation to assure that documents are being preserved and that the client understands the ramifications if evidence is lost or destroyed. If neither Little Fish nor its counsel has the sophistication to guide the client, then obtaining expertise is mandatory.
    - Little Fish may not have the resources in place to effect proper *e*-document retention program.
    - Client costs become an issue:
        - direction and supervision by legal counsel,
        - acquisition of additional or new technology, both software and hardware, may be required, and
        - engagement of IT professionals may be required to assure compliance.

[5] Courts usually require the suspension of routine document retention/destruction policies, which is sometimes referred to as a "litigation hold." This includes the recycling of backup tapes and other backup media. See *Zubulake IV*, 220 FRD at 218.

- **Communicate directly with the "key players".** Little Fish may not have key players other than the officers of the company or the client itself. But in communicating with key players, counsel must be assured that the key players are knowledgeable about the requirements to preserve *e*-data and how to do it.
    - Little Fish may not have an IT department or even an IT person, therefore:
        - client must be able to preserve *e*-data; that is know how to retain the information on the client's computers; if not, hire an outside consultant and
        - client must have the appropriate hardware and software to permit preservation.
    - Both Client and Counsel must have discussed all of the various equipment and locations where *e*-data can be found:
        - personal/home computers,
        - portable computers,
        - PDA, cellular telephones, and other storage communication devices, and
        - stored media: flash cards, USB cards, Memory Sticks

        .

Little Fish may be more exposed to *e*-data proliferation as many small businesses and individuals have no rules governing the use of company and/or personal computers. Relevant *e*-data may reside almost anywhere; hence relevant, "accessible" data will most often be disbursed across all types of media and locations that would otherwise be controlled by a Big Fish. This makes preservation over relevant information more difficult and places greater responsibility on counsel to make sure that the client has preserved all of the *e*-data that exists.

Do not hesitate to call in a consultant that is knowledgeable about computers and *e*-data storage. Loss of *e*-data is common and can occur easily. The cost to the client will out weigh the risk of making a mistake during *e*-discovery. Discovery errors that lead to sanctions against the client could also lead to claims of malpractice against the lawyer.

As to what must be retained, Judge Scheindlin comments in *Zubulake IV* [6]:

> "A party or anticipated party must retain all relevant documents (but not multiple identical copies) in existence at the time the duty to preserve attaches, and any relevant documents created thereafter. In recognition of the fact that there are many ways to manage electronic data, litigants are

[6] 220 F.R.D. at 218

free to choose how this task is accomplished. For example, a litigant could choose to retain all then-existing backup tapes for the relevant personnel (if such tapes store data by 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 system 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. Presumably there are a multitude of other ways to achieve the same result." (Emphasis supplied)

Caveat: Unless you are absolutely certain that the client has sequestered all relevant *e*-data and has it fully backed up, making a mirror image of the client's computers is essential at the time the duty to preserve arises. Important, too, is to make absolutely sure that the back up systems exist and are working and in good order to avoid the subsequent loss of *e*-data. New or additional hardware and software may have to be acquired by the client to achieve assurance that *e*-data will not be lost. The client must be fully versed in preserving *e*-data, however it is kept and wherever it maybe stored

For example:

- Emails on AOL or Outlook are automatically archived on most computers. Can the email be recovered and will the attachments still be attached. Leaving emails on a server can result in automatic destruction without any ill intention simply because they were archived. Little Fish are unlikely to have sophisticated systems in place to store emails and other information, relying, more likely, on esp. providers to provide archival services.
- Hard drives crash without warning and recovery of data will be expensive and may be made impossible for certain types of databases. (QuickBooks is a good example of a difficult data base to restore.) A mirror image of the client's computer system is essential in protecting loss of *e*-data.
- Back up tapes or other back up media can be written over easily and critical back up of relevant *e*-data lost. Little Fish may believe that the back up system is working and back up procedures are being followed only to learn when a back up is to be restored that the system failed due to human error.

Produce electronic copies of their relevant active files. Sounds easy but is it? Counsel may be required to produce *e*-data in its native format with all of the Meta-information intact. If either you or your client are fully competent to capture and reproduce *e*-data, and have the equipment and the software to do it, don't. Well meaning but unskillful efforts can result in the loss of *e-data*, or critical aspects of it, and that will be hard to explain to the Court in response to a motion to compel.

E. Will Rule 37(f) Offer Safe Harbor to Little Fish that Make a Mistake? No I Do Not Think So

Proposed FRCP 37(f) addresses "the routine alteration and deletion of" electronically stored information that can occur automatically without an operator's direction or knowledge. These automatic alteration and deletion features arguably may result in an innocent party losing

potentially discoverable information; however, once the duty to preserve attaches to your client's *e*-data, there is really no innocent failure to preserve as all routine conduct is suspended under a *litigation hold* requirement: "Once a party reasonably anticipates litigation, it must suspend its routine document retention/destruction policy and put in place a "litigation hold" to ensure the preservation of relevant documents." *Zubulake IV*, 220 F.R.D. at 218.

Little Fish may not be troubled by routine document retention/destruction policies as it may have none. Therefore, any loss of *e*-data may fall outside of a safe harbor. The loss of *e*-data from human error under the findings of Judge Scheindlin in *Zubulake V* (229 F.R.D. at 435) are not forgiving of missteps, particularly on the part of lawyers:

> On the other hand, UBS's counsel are not entirely blameless. "While, of course, it is true that counsel need not supervise every step of the document production process and may rely on their clients in some respects," [footnote eliminated] counsel is responsible for coordinating her client's discovery efforts. In this case, counsel failed to properly oversee UBS in a number of important ways, both in terms of its duty to locate relevant information and its duty to preserve and timely produce that information.

The risk to the lawyer representing a Little Fish is that in making the communication, the gap of understanding and sophistication is sufficiently large that the client fails to understand the gravity of the duties to preserve and produce *e*-data. An adverse inference against a client points a finger at the lawyer too.

CONCLUSION

All of the rules regarding the preservation and production of *e*-data apply to Little Fish. However, the risks, of *e*-data loss is often much greater for Little Fish as they lack the sophistication, internal controls and infrastructure to protect themselves from the requirements of the Rules of Civil Procedure that will apply to *e*-discovery.