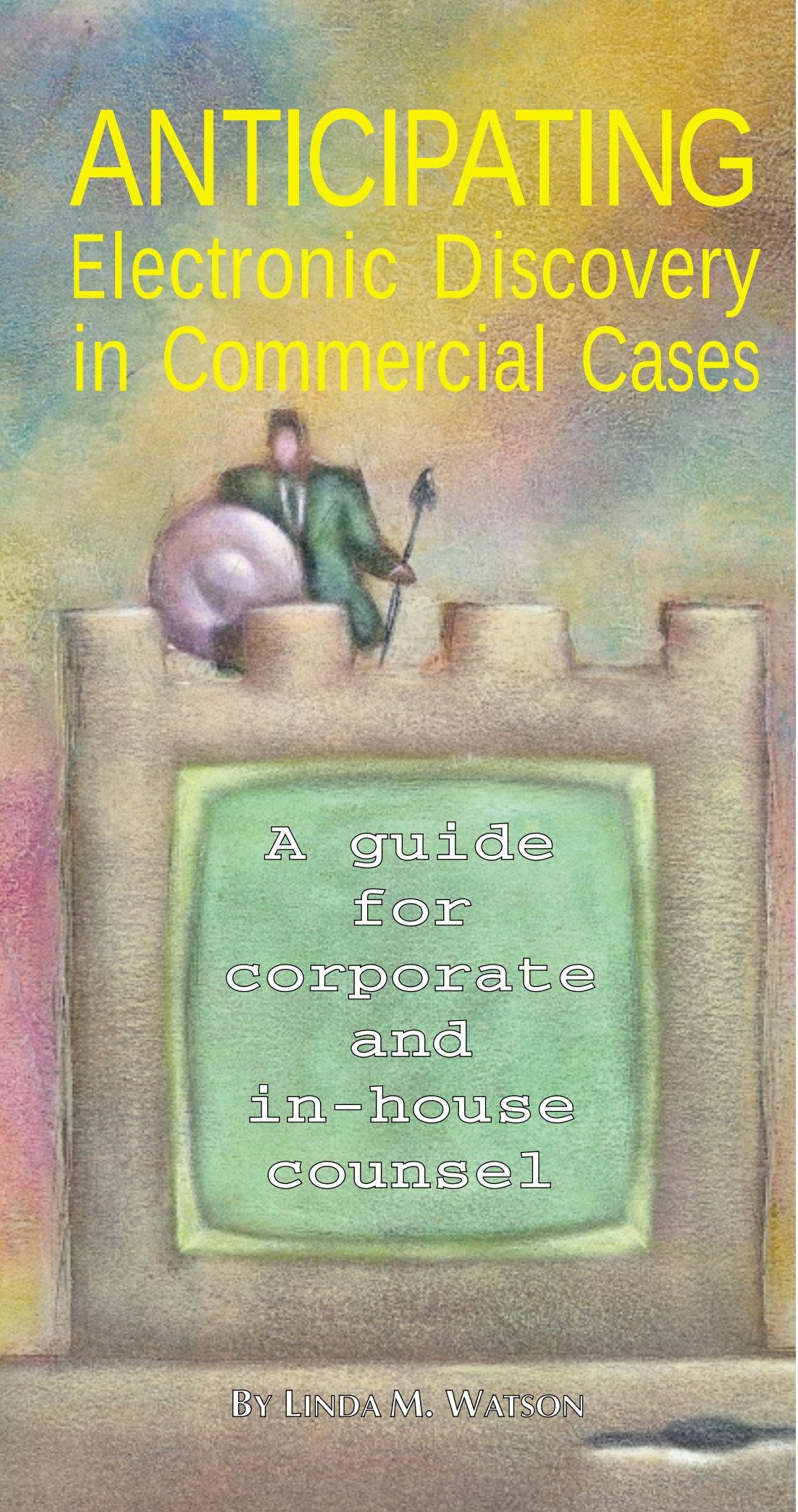


Discovery has moved into the electronic age. E-mail and electronic files are both prolific and virtual. Indeed, e-mail use has grown in leaps and bounds in the last 10 years, and is now a primary form of business communication.[1] Unfortunately, it is often used casually and conversationally, with many users believing that their messages are quickly deleted.[2] This mistaken belief often results in a proverbial "smoking gun."

Case in point—a central focus of the Martha Stewart trial was that the "Domestic Diva" altered an electronically recorded phone message from her broker, then had her personal assistant restore the message to its original form. Ms. Stewart's assistant testified she located the original in a back-up file. Had the message not been restored by Ms. Stewart's assistant, it is likely that the prosecution would have discovered the original message in the back-up file on its own—the "smoking gun." Could such an e-mail or electronic file be sitting out there on your network?

Imagine being a party in a commercial dispute and receiving document requests demanding production of back-up tapes containing any material relating to the subject litigation, exact copies of all hard drives on desktops, laptops, and notebooks, and exact image copies of relevant diskettes. Are you prepared to respond? Before your company or client becomes the subject of an electronic discovery request (or before you initiate one, since the favor will definitely be returned), you need to know if your company is ready and, if not, how to prepare. This article will address:

- how courts currently treat electronic discovery requests
- shifting the cost of electronic discovery
- the pitfalls of spoliation—what every company needs to avoid
- how to get your digital house in order

THE CURRENT STATE OF ELECTRONIC DISCOVERY

The discovery of electronic data is critical in today's commercial case because a significant number of electronically stored documents are never reduced to print,[3] including databases, e-mail, word processing and presentation files, spreadsheets, CAD/CAM/CAE and graphics, personnel records, policy and procedure manuals, among others.[4]

The discovery of electronic media is governed by Rules 26 and 34 of the Federal Rules of Civil Procedure. Rule 26(a) provides for initial disclosures of "all documents, data compilations, and tangible things" that the disclosing party may use to support its claims or defenses. Rule 34 broadly defines "documents" as including electronic data.[5]

In Michigan state courts, electronic discovery is governed by MCR 2.302, which provides for discovery of "any matter, not privileged, which is relevant . . . including . . . documents or other tangible things . . . ," and MCR 2.310, which provides for the production of documents, including:

> *writings, drawings, graphs, charts, photographs, phono records, and other data compilations from information can be obtained, translated, if necessary, by the respondent through detection devices into reasonably usable form.*
>
> MCR 2.310(A)(1).

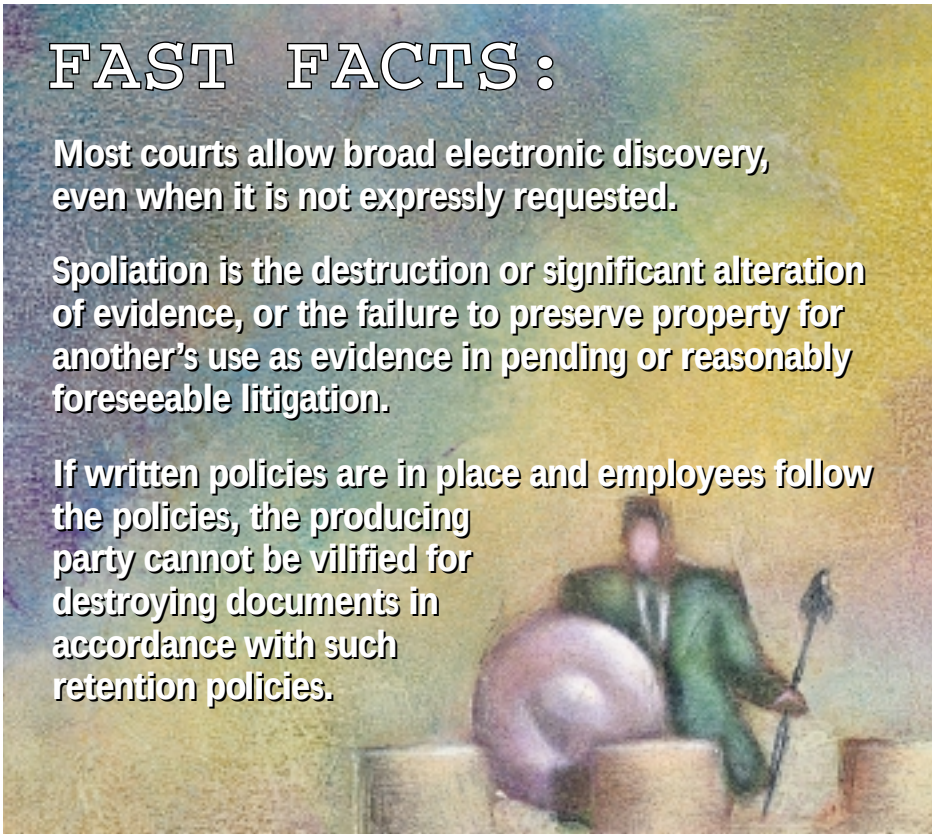
After the adoption of the 1970 Amendment to Rule 34, few courts have found authority to rule against the discoverability of information simply because it was stored electronically. Indeed, most courts allow broad electronic discovery, even when it is not expressly requested. For example, in *Playboy Enterprises, Inc v Terri Welles*,[6] Playboy sued a former Playmate of the Year for trademark infringement and petitioned the court to grant access to the hard drive of her personal computer to recover deleted e-mail.[7] The defendant argued the request was defective for failure to specifically mention e-mail or computer hard drive in its text.[8] The court found that by requesting "documents," the plaintiff had effectively requested production of information stored in electronic form. The rationale was that any e-mail found in the defendant's hard drive would have to be produced as a document and therefore e-mail should be construed as documents.[9] The rest of the plaintiff's requests were simply discoverable under Rule 34 and Rule 26 and the plaintiff was allowed access to create a mirror image of the defendant's computer hard drive.[10]

COST-SHIFTING

Relying on traditional discovery tools of control, courts have afforded protection from abusive requests for electronic discovery. Above and beyond the standard protective order, a court may protect the responding party from "undue burden or expense" by shifting some or all of the costs of production to the requesting party.[11] Whether a cost is an undue burden is decided on a case-by-case basis. If the total cost is not substantial, the responding party will likely accept the expense. This leads to the ultimate question: what is a substantial cost and how should the courts quantify an undue burden?

One of the most recent cases on this issue is *Zubulake v UBS Warburg LLC*,[12] where the court opined that the scope and cost of discovery of electronic data required a three-step analysis.[13] The first step is to understand the responding party's computer system with respect to active and stored data. Importantly, the court opined that for "data kept in an accessible format, the usual rules of discovery apply: the responding party should pay the costs of producing responsive data. Thus, a court should consider cost-shifting only when electronic data is relatively inaccessible, such as in back-up tapes."[14]

The second step is to determine what data may be found on the inaccessible media, which requires the responsive party to produce a small sample of the requested back-up tapes.[15] The *Zubulake* court ordered the defendant to produce five back-up tapes as a sample.



The third step in conducting the cost-shifting analysis is to consider the following factors weighted more or less in the following order:

- the extent to which the request is specifically tailored to discover relevant information
- the availability of such information from other sources
- the total cost of production, compared to the amount in controversy
- the total cost of production, compared to the resources available to each party
- the relative ability of each party to control costs and its incentive to do so
- the importance of the issues at stake in the litigation
- the relative benefits to the parties of obtaining the information[16]

Once it analyzed the sample and applied the above factors, the *Zubulake* court determined that the cost of restoring and searching any back-up tapes, which cost was estimated to be $273,649.39,[17] should be allocated between the plaintiff (the party requesting the discovery) and the defendant 75 percent and 25 percent, respectively. The court ordered all other costs to be borne exclusively by the defendant.[18]

In addition to *Zubulake*, courts have developed a variety of tests in order to decide cost-shifting. The tests, unlike that in *Zubulake*, usually favor defendants. For example, in *McPeek v Ashcroft*, the plaintiff tried to compel the Department of Justice to produce the entirety of its back-up systems to find deleted e-mail. The court struggled with a way to be "fair" to both parties given the breadth of Rule 34 and the constraints of Rule 26.[19] The court likened the plaintiff's request to, "[trying to find] an awfully expensive needle to justify searching a haystack."[20] The court employed a marginal utility philosophy to settle the dispute. It deemed that this approach would place the burden on the plaintiff because it was not likely that it would find anything of value in what was being produced and it was inequitable to the defendant to force it to produce the materials.[21]

Likewise, in *Rowe Entertainment, Inc v The William Morris Agency, Inc*,[22] a group of concert promoters sued several talent agencies for allegedly freezing them out of the market of promoting certain events.[23] The plaintiffs moved for production of all documents, including e-mail, concerning any communication between any of the defendants relating to the selection of concert promoters in the course of its business.[24] The William Morris agency alone estimated that to fulfill the plaintiffs' discovery request would cost approximately $9,750,000.[25] The court employed an eight-factor balancing test.[26] Using this system, the court shifted all costs of production to the plaintiff, save that of the defendants' search of their own materials for privileged e-mails, finding that although the plaintiff could not obtain the information by other means, the plaintiff's discovery requests were very broad and the plaintiff had not been able to prove that e-mail discovery would be a "goldmine" of relevant information.[27]

THE PITFALLS OF SPOLIATION

"As documents are increasingly maintained electronically, it has become easier to delete or tamper with evidence (both intentionally and inadvertently) and more difficult for litigants to craft policies that ensure all relevant documents are preserved."[28] A duty to preserve arises at the time that litigation was reasonably anticipated.[29] Spoliation is "the destruction or significant alteration of evidence, or the failure to preserve property for another's use as evidence in pending or reasonably foreseeable litigation."

While a party need not preserve all back-up tapes, it has a duty to "preserve what 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."[30] This duty extends to those employees likely to have relevant information—"the key players."[31]

If a party plans on requesting electronic evidence, it should send a preservation of evidence letter to the responding party at its earliest opportunity.[32] The notice should identify the types of information to be preserved. As to a responding party, once litigation is anticipated, a preservation directive should be issued to, and adhered to by, key players. When litigation begins, the requesting party should take the next step and obtain a protective order requiring all parties to preserve electronic evidence.[33]

If spoliation occurs, the court may impose sanctions, including reconsideration of cost-shifting, an adverse inference instruction at trial, or a default judgment, among other things. In *Crown Life Ins Co v Craig*,[34] an insurance company that failed to produce electronic data was sanctioned in that it was not allowed to present certain evidence and defenses. In *Kucala Enterprises, Ltd v Auto Wax Company, Inc*,[35] the plaintiff's case was dismissed and the plaintiff ordered to pay attorney fees and costs after it was determined that the plaintiff used a computer program called "Evidence Eliminator" to delete documents from his computer after litigation had begun "in wee hours" of the morning, just before the defendant's computer specialist was to take an image of the plaintiff's computer.

GETTING YOUR DIGITAL HOUSE IN ORDER

There are a number of steps a company can take to manage risk as it relates to electronic discovery and the potential for smoking guns, cost-shifting, and spoliation. Below are some tips for getting your company prepared for the next case.

Develop, implement, and follow policies and procedures on the retention of digital or electronic data.

It is a common misconception that deleting e-mail or documents on your computer destroys them forever. Indeed, the file is lodged in the unallocated space of the hard drive. An examination by a computer forensics team of a bit stream copy of this space will reveal the contents of the document or e-mail.[36]

If written policies are in place and employees follow the policies, the producing

party cannot be vilified for destroying documents in accordance with such retention policies. Therefore, counsel should work with the company's Information and Technology Department to prepare policies and procedures on how long e-mails are to be retained before being deleted and how long back-up information is going to be stored.

Some experts recommend a policy that requires e-mails to be automatically erased, including back-ups, after a short period of time such as 15–30 days.[37] There is software that can be purchased that imposes records retention discipline in that they automatically erase e-mail messages after the defined period of time.

Companies can also create and enforce policies on writing standards as to e-mail. More specifically, a company can provide a feature, such as formal letterhead for certain e-mails, so that they are characterized as an official company record or an official position of the company, as opposed to less formal e-mails that are not intended as official records or positions of the company.[38]

Organize how electronic information is preserved or hire reputable companies to do it.

Physically segregating the back-up copies of the e-mail system from back-ups of the rest of the computer system will make it easier to respond to discovery requests seeking electronic evidence.[39] For example, administrative documentation is placed on a back-up tape separate from correspondence. Or, a company can maintain its e-mail on one computer system or network.

Develop a digital electronic discovery response program.

In a recent survey, more than 80 percent of companies did not have an established protocol for handling electronic discovery requests.[40] Indeed, most corporate IT departments, while technically capable, are scaled for ongoing operations, and are not prepared to handle discovery of electronic data.[41] A response team should be comprised of individuals from various departments within the organization such as Human Resources, Information and Technology, Administrative, and Legal. The goal should be to incorporate necessary retention requirements with organizational needs to establish not only a retention policy, but in what fashion documents will be stored or organized.

Educate employees on their use of e-mail.

One of the best steps a corporation can take is to educate its employees on the potential immortality of e-mail. E-mail has become a very informal and sometimes hasty way of communicating. Employees think that when they delete an e-mail from their computers, it is gone and erased for good. This is anything, but true. E-mail, even when deleted, is not actually destroyed once and for all until it is actually written over. That may never happen. Employees need to understand that e-mail is not private. It may have been quick idle chit-chat one afternoon, but an official record of the organization on the day of trial.

RESPONDING TO DIGITAL EVIDENCE DISCOVERY REQUESTS

If you receive discovery requests seeking digital evidence, there are a number of steps that should be taken in order to prevent or at least limit discovery, and perhaps shift some or all of the costs.

1. Obtain a Protective Order to limit the scope of the request and to protect documents that contain privileged communications such as the attorney/client privilege or the physician/patient privilege. This may also be a good time to agree to a protocol and to extend time periods for responding to discovery.
2. Preserve Electronic Data by taking steps to stop the automatic overwriting processes for relevant electronic data upon receipt of a notice that a lawsuit may be filed or has been filed. Also, as indicated above, a directive should be issued to key employees to preserve electronic evidence. Well over 50 percent of companies surveyed responded that they either never or rarely take preservation steps.[42] As discussed above, this often leads to spoliation.
3. Shift the Cost of Responding to the requesting party if the electronic data is not accessible and it will be costly to search and recover. A company may want to retain a computer forensic expert to assist in determining where the requested information is located, if it is accessible, what kind of labor and money it will take, as well as time, to search and recover the electronic data and if the data will still need to be translated. The expert can provide an affidavit, which is extremely compelling, to submit with a motion or petition to shift the cost of responding. Likewise, parties requesting electronic data will often retain an expert to assist them in launching a cyber attack of electronic discovery requests. Qualified computer experts should be prepared to help educate and navigate.[43]
4. Avoid Mishandling by preserving the chain of custody. If you are producing electronic evidence, be prepared to demonstrate that (1) no information has been added or modified, (2) a complete copy was made, (3) a reliable copying process was used and (4) all media was secured.[44] This is where an expert can prove invaluable and testify at trial about a clean chain of custody.

Discovery of electronic evidence can become a company's worst nightmare if it is not prepared to handle the requests. Litigants are counting on this type of disarray to take the advantage and make your next commercial case a procedural and substantive landmine. With a little effort now, your company can avoid an emergency situation. ✦

Linda M. Watson is a partner at Cox, Hodgman & Giarmarco, P.C. and concentrates her practice in the areas of contract disputes, business torts, employment law, trade secret violations, competition lawsuits, and shareholder actions, as well as patent litigation support and trademark challenges. Ms. Watson was co-theme-editor of this Michigan Bar Journal *issue and would like to thank Jonathon Rosenthal for his assistance in writing this article.*

FOOTNOTES

1. E-mail: The smoking gun of the future, Patricia Nieuwenhuizen, The National Law Journal, December 11, 2000. In 2000, office workers exchanged 25 billion e-mail messages daily.
2. Id.
3. Id. In the year 2000, experts advised that "30 percent of electronically stored documents are never printed to paper."
4. Areas of Consideration for E-Evidence, CyberControls, L.L.C., 2004.
5. Electronic data was added by way of the 1970 Amendment to Rule 34.
6. 60 F Supp 2d 1050 (1999).
7. Id.
8. Id. at 6.
9. Id. at 9.
10. Id. at 14.
11. See FR Civ P 26(c).
12. 2003 U.S. LEXIS 7939, May 13, 2003.
13. Id.
14. Id. at 49–50. The court ordered the defendant to produce all e-mails that existed on its optical disks and active servers at its own expense since it was in an accessible format.
15. Id. at 50.
16. Id.
17. *Zubulake v UBS Warburg LLC*, 216 FRD 280, 289–290 (So Dis NY 2003). The estimated cost of producing the information included restoration of the remaining back-up tapes, searching costs and attorney and paralegal costs.
18. *Zubulake v UBS Warburg, LLC*, 216 FRD 280; 2003 U.S. Dist. LEXIS 12643 (July 24, 2003).
19. Id. at 32.
20. Id. at 34.
21. Id.
22. *Rowe Entertainment, Inc v The William Morris Agency*, 205 FRD 421 (2002).
23. Id. at 423.
24. Id. at 424.
25. Id. at 425.
26. Id. at 429–430. The factors are as follows: (1) the specificity of the discovery requests; (2) the likelihood of discovering critical information; (3) the availability of such information from other sources; (4) the purpose for which the responding party maintains the requested data; (5) the relative benefit to the parties of obtaining the information; (6) the total cost associated with the production; (7) the relative ability of each party to control costs and its incentive to do so; and (8) the resources available to each party. Each factor was weighted, but with the lower factors (1, 2 and 3) carrying more influence than the higher numbered factors, even though all were considered important.
27. Id.
28. *Zubulake v UBS Warburg LLC*, 2003 U.S. Dist. LEXIS 18771; 92 Fair Empl. Prac. Cas (BNA) 1539 (United States District Court for the Southern District of New York) (October 22, 2003).
29. Id. at 11. (The court found that almost everyone associated with the plaintiff recognized the possibility that she might sue and held that the duty to preserve arose long before the EEOC claim was filed and the litigation began.)
30. Id. at 13.
31. Id. at 14.
32. Collecting Computer-Based Evidence, Joan E. Feldman and Rodger I. Kohn, New York Law Journal, January 26, 1998.
33. Essentials of Electronic Discovery, Finding a Using Cyber Evidence, Joan E. Feldman, 2003, page 6-27.
34. 995 F2d 1376 (CA 7, 1993).
35. 2003 U.S. Dist. LEXIS 8833; 56 Fed R Serv 3d (Callaghan) 487 (Northern District of Ill Eastern Division) (May 23, 2003).
36. The Progressive Stages of a Digital Evidence Discovery Engagement for Plaintiff's Attorneys by CyberControls, L.L.C., 2004.
37. Discovery and Destruction of E-mail, Donald S. Skupsky, Chapter 5 at page 15.
38. Id.
39. Id.
40. PricewaterhouseCoopers/Section of Litigation of the American Bar Association Pulse Survey, Digital Discovery and its Importance on the Practice of Litigation.
41. Areas of Consideration for E-Evidence, CyberControls, L.L.C., 2004.
42. PricewaterhouseCoopers/Section of Litigation of the American Bar Association Pulse Survey, Digital Discovery and its Importance on the Practice of Litigation.
43. Planning and Conducting Electronic Discovery, Joan E. Feldman, 2003 at page 6-25. See also the qualifications and services to look for in an expert at page 6-25 through 6-26.
44. Planning and Conducting Electronic Discovery, Joan E. Feldman, 2003 at page 6-30.