TABLE OF CONTENTS

I. INTRODUCTION 2

II. MY APPROACH 3

III. THE HORROR STORIES 3

IV. THE I.T. ASPECT 4

V. ATTORNEY CLIENT PRIVILEGE CONSIDERATIONS 5

VI. OPEN MEETING – GOVERNMENT IN THE SUNSHINE VIOLATIONS 6

VII. LITIGATION AND DISCOVERY RULE 26 OBLIGATIONS 8

VIII. SPOLIATION OF EVIDENCE AND SANCTIONS 10

IX. COSTS 12

X. RISK MANAGEMENT 13

XI. WHAT YOU SHOULD DO AND WHEN YOU SHOULD DO IT 14

I.
INTRODUCTION

Is your City Normal? "Normal" in the sense of being comparable to other city governments (or for that matter, private corporations) and similarly situated to its sister cities within your state and our nation? If so, you already know -or will soon discover- that it is either incompetent or ineffectual, or both, in its understanding and performance of its duties under the law with respect to electronic documents and email. There is true opportunity for you here to make a difference, avoid a disaster or two, and even be a hero.

This reality – and it truly is a reality – does not necessarily mean that your city is a part of the axis of evil. In many cities, there has been a delayed technology, and in implementing it by way of policy, practice, and habit. However, the excuses that have succeeded in the past are rapidly disappearing as Judge Shira A. Shinelan states in a recent post script in her recent ruling concerning email discovery defaults in July of this summer:

> "The subject of the discovery of electronically stored information is rapidly evolving. When this case began more that two years ago, there was little guidance from the judiciary, bar associations or the academy as to the governing standards. Much has changed in that time. There has been a flood of recent opinions – including a number from appellate courts – and there are now several treatises on the subject.[1] In addition, professional groups such as the American Bar Association and the Sedona Conference have provided very useful guidance and thorny issues relating to the discovery of electronically stored information.[2] Many courts have adopted, or are considering adopting, local rules addressing the subject.[3] Most recently, the Standing Committee on Rules and Procedures has approved for publication and public comment a proposal for revisions to the Federal Rules of Civil Procedure designed to address any of the issues raised by the discovery of electronically stored information.[4] Now that the key issues have been addressed and national standards are developing, parties and their counsel are fully on notice of their responsibility to preserve and produce electronically stored information. The tedious and difficult fact finding encompassed in this opinion and others like it is a great burden on a court's limited resources. The time and effort spent by counsel to litigate these issues has also been time-consuming and distracting.

---

[1] *See* MICHAEL ARKFELD, ELECTRONICE DISCOVERY AND EVIDENCE (2003); ADAM I. COHEN & DAVID J. LENDER, ELECTRONIC DISCOVERY: LAW AND PRACTICE (2004)

[2] Memorandum from Gregory P. Joseph & Barry F. McNeil, *Electronic Discovery Standards – Draft Amendments to ABA Civil Discovery Standards* (Nov. 17, 2003); The Sedona Conference, *The Sedona Principle: Best Practices Recommendations & Principles for Addressing Electronic Document Production* (January 2004), available at http://www.thedonaconference.org/publications-html. See attachment.

[3] *See also* Memorandum from the Ninth Circuit Advisory Boards, *Proposed Model Local Rules on Electronic Discovery,* available at http://www.krollontrack.com, D.Kan.*Electronic Discovery Guidelines;* D. Del. *Default Standards for Discovery of Electronic Documents.*
http://www.kenwithers.com/rulemaking

[4] http://www.kenwithers.com/rulemaking/civilrules/report051704.pdf.

> This Court, for one, is optimistic that with the guidance now provided it will not be necessary to spend this amount of time again. It is hoped that counsel will heed the guidance provided by these resources and will work to ensure that preservation, production and spoliation issues are limited, if not eliminated."

II.
MY APPROACH

This is a resource paper. There will be a limited amount of narrative material, for two reasons. Number one, you wouldn't read it anyway. Number two, this paper has been developed as a tool or starting point for municipal law professionals seeking a prompt grasp of the law and technology necessary to play a proactive role in their organization. Moving forward toward compliance with the law, and the effective and knowledgeable management of the electronic information resources, which are so powerful, but can be so problematic.

III.
THE HORROR STORIES

You truly don't know how vulnerable you are, unless you have already been one of the victims of email mistakes or sanctions in litigation. Here are some examples from our recent experiences, and from the headlines in both the media at large and the legal profession media:

- Imposition of sanctions in the amount of $2,995,000, together with the exclusion of testimony by any fact or expert witness who has failed to comply with Phillip Morris Internal Document Retention Program;
- The imposition of a judgment of liability, together sanctions and costs against both the defendants and their counsel in the case *Metropolitan Opera Ass'n, Inc. v. Local 100, Hotel Employees and Restaurant Employees Intern. Union*, 2004 WL 1943099 (S.D.N.Y.) for failing to carry out the joint responsibilities under the law to identify, obtain, retain, and produce email in discovery;
- The imposition of an adverse inference instruction at trial (see appendix A), together with the imposition of costs of production, of re-deposing witnesses, of evidence and back up tape restoration together with the associated costs and fees; and
- Potential exposure to criminal sanctions for violation of the open meetings or government in the sunshine law pertaining to public deliberations.
- Public disclosure of documents retained by elective officials on their home computers, including email communications and correspondence which may touch and concern city business issues.
- Libel lawsuit against a city arising out of statements by the city's CPR coordinator made in a stray email regarding a contracted CPR technician's certification to teach under the auspices of the American Heart Association. Though the email was held not to be libelous, the lawsuit may never have occurred if the city had kept a tighter rein on its email.

IV.
THE I.T. ASPECT

Generally, computer software programs keep track of the location of files by storing that information in a file allocation table. This information resides on the computer or server hard disk. The apparent location of the material shown on the computer display on the screen is a user convention. The file allocation table facilitates access to sites on the disk where the data is actually located. When the file is "deleted", it is usually not deleted. Some programs refer to this first phase of deletion as a "trash bin" or a "recycle bin." Even when files are deleted or emptied from those locations, the data still remains on the hard disk, until it has been overwritten. The over-writing process may be gradual or incomplete. Even when portions of the data have been overwritten, the underlying original information may be subject to restoration or recovery, either in whole or in part. Even when all of the information is no longer available, information about who changed, deleted, or otherwise modified or accessed it, and when those things occurred, may yet be available.

Determining the extent of a duty or obligation to produce stored electronic information required starts with what level of stored access is required. Under the Texas Open Records Act, deletion of material from the "recycle bin" means that it is no longer being maintained by the government, so it is no longer public information.[5] That is typically not the result in litigation, especially where the obligation to retain that information arose prior to the time of deletion. See the litigation discussions below.

The problem is not as simple as dealing with the workstations, networks and servers at City Hall or other places of public work. As one court dealing with this issue has observed:

> "Courts also have recognized, however, that requests to discover electronically stored information do not have the same impact on the receiving party as do those requests for "hard copy" records. For example, the scope of what is included in the phrase "electronic records" can be enormous, encompassing voice mail, **email**, deleted **email**, data files, program files, back-up files, archival tapes, temporary files, system history files, web site information in textual graphical or audio format, web site files, cache files, "cookies" and other electronically stored information. *Kleiner v. Burns*, 2000 WL 1909470 (D.Kan.). According to one study, "93% of all information generated during 1999 was generated in digital form, on computers. Only 7% of information originated in other media, such as paper. *In re Bristol-Myers Sauibb Securities Litigation,* 205 F.R.D. 437, 440 n.2. (D.N.J., 2002)
>
> Thus, searching for deleted electronic records can be particularly time consuming and expensive given the number of storage locations that may have to be checked (e.g., desk-top computer, laptops, PDA's, data, and system files, for instance), coupled with the possible need to use special search methods to locate deleted files."

[5] Texas Government Code §552.002; Tex. Att'y Gen. Or 2000-2326

V.
ATTORNEY CLIENT PRIVILEGE CONSIDERATIONS

Preservation of the attorney client privilege requires attention and training as much as it requires knowledge of the law. The loss of the privilege usually results from carelessness. When you get home, start the process of training and educating those within your organization to preserve the privilege. Make sure that your program includes the "Expect what you inspect" principle. In other words, ask, remind and discuss the standards during the daily communication process to test and confirm that people are doing this correctly.

EXAMPLE:

We are here today to go over the draft agreement with the paving contractor on this bid from the meeting last week, and I sent each of you my updated draft with comments on Friday. Before we start, let me just check with you all to make sure that everyone understands and is following the protocols on the AC Privilege that our office promulgated last year. Does everyone have a copy? No one has distributed the comments or evaluations outside of the original distribution list on my email and bin mail, correct? Does everyone understand that we have to keep this within the actual decision-making circle in order to preserve the privileges for the City? Just so it is clear, that means that we can't send the bidder our comments and see what they think; we can't read them over the phone and get their reaction; we can't take their calls about why their lawyers say we don't have to require that paragraph and explain what your lawyer says to the contrary. Any questions about how that all works? Otherwise, we might as well just go over and have this talk in their conference room and sit around naked together."

Labeling all communications with lawyers, --from Jokes, to lunch plans, to weekend family reports-- as CONFIDENTIAL ATTORNEY CLIENT COMMUNICATION … ETC. is not a good idea. It makes it easy to prove a lack of attention and diligence when the inevitable battle occurs. Including the AC NOTICE is required practice, but if the client is going to hand it out at a public meeting, what's the point? Only use it on truly private communications. The best system is one that requires the sender to elect whether that notice is included on emails. The NOTICE should also make it clear that the communication is not subject to release or authorized for **forwarding** without consultation with the lawyer/author.

Whether the transmission and residence of email in the I.T. systems and servers of third parties is a disclosure that waives the privilege has been discussed. However, it is currently accepted that an appropriate level of diligence for actual non-disclosure to third party users (as opposed to system techs that may have theoretical access) coupled with a notice, is sufficient to maintain a confidential status.

> "The contents of this message may be confidential and subject to the attorney/client privilege. If you are not the intended recipient(s) of this message, please destroy this message immediately. No permission is given for persons other that the intended recipient(s) to read or disclose the contents of this message."

The American Bar Association approved this method as sufficient to protect confidential information transmitted via email, so long as the lawyer has consulted with his or her client as to the acceptability of transmitting information in this manner.

For the privilege to apply:

1. the holder must be (or have sought to become) a client;
2. the person to whom the communication was made must be an attorney acting as such at the time;
3. the communications must be made in confidence; and
4. the communications must be made for the purpose of receiving legal assistance.

American Bar Association Formal Ethics Opinion 99-413 (1999).

TEX.R.EVID 503

Effective March 1, 1998, Rule of Evidence 503 was amended to adopt the "subject matter" test for an entity's assertion of the privilege, replacing the "control group" test previously used. *Nation Tank Co. v. Brotherton,* 851 S.W.2d 193, 197-98 (Tex. 1993). We recommend that you determine the applicable standard in your jurisdiction and draft a policy and procedure in compliance with it. All issues concerning the attorney client privilege should be reduced to an official policy or an ordinance. It makes the lawyer's "policeman" role more comfortable and effectual for the lawyers. It may even add force to your argument in the future that disclosures by persons not authorized to act for the governing body should not be given effect, to the ultimate disadvantage of the taxpaying citizen members of the body politic.

See the discussion of copy lists and attorney client privilege in *re Avantel*, 343 F.3d 311, 316 (5th Cir, 2003).

VI.
OPEN MEETING – GOVERNMENT IN THE SUNSHINE VIOLATIONS

In any municipal government environment, the day-to-day issue for electronic information is the Public Information Act question. Issues will also arise about whether decisions have come about by virtue of electronic communications, rather than where required in public forums with required statutory notice. Under these statutes, information in electronic form can have a dynamic impact.[6] The legal tasks associated with those issues include not only making the determinations based on prior acts and communications, but hopefully the positive influencing of behavior and practices which make the outcomes more likely palatable, and less likely sanctionable or worse.

Some excellent suggestions toward that positive influence are these from Alan Bojorquez:

---

5 See Jay Doegey and Elizabeth Lutton: International Municipal Lawyers Association magazine; "To: Council Members, Re: You've Got Email, Message: Think Before You Reply," from the *Municipal Lawyer*, January/February 2002, Vo. 43, No.1.

1. Evaluate the sensitivity of the communication and the potential costs of inadvertent disclosure.
2. Don't say anything in an email that you would not print on letterhead and sign your name to.
3. Be descriptive in the "subject" line.
4. Try to limit the message to a single subject.
5. Use caution when instinctively replying to a message you have received.
6. Avoid airing disputes over email.
7. Be selective when copying or blind copying other recipients on a message.
8. Be deliberate when forwarding emails.
9. Protect privileged or confidential information
10. Diligently maintain your files and clean your system regularly.
11. Understand that employers can inspect employee email in certain situations.
12. Remember that if you want to withhold an email that is responsive to an public information request, you must submit the document to the attorney general to determine if it is privileged, confidential, or subject to an exception.

To use our most familiar examples for your, consider the Texas Public Information Act (TPIA). The preamble declares that "It is the policy of this state that each person is entitled, unless otherwise expressly provided by law, at all times to complete information about the affairs of government and the official acts of public officials and employees."

Section 552.137(a) of the TPIA provides that an email address of a member of the public used for the purpose of communicating with a governmental body is confidential and not subject to disclosure. This means that the government must seek to protect this information, unless the member of the public has affirmatively consented to its release.

Section 552.002(a) of the TPIA defines public information as "information that is collected, assembled, or maintained under a law or ordinance or in connection with the transaction of official business:

1. by a governmental body; or
2. for a governmental body and the governmental body owns the information or has a right of access to it.

These provisions seem to have cross purposes or outcomes. Is it only the information of the governing body that is public or every home email that the Mayor writes that touches any issue of city government?

Tex. Att'y Gen. OR 2001 – 1790 cites Tex. Att'y Gen. ORD-635 (1995) for the proposition that:

> "Records that [are] clearly related to official business are public records subject to the act regardless of whether an individual member of a governmental body, the governmental body's administrative offices, or the

> custodian of records holds the records. If a governmental body could withhold records relating to official business simply because they are held by an individual member of the governmental body, it could easily and with impunity circumvent the act merely by placing all records relating to official business in the custody of an individual member. The legislature could not have intended to permit governmental bodies to escape the requirement of the act so easily."

Another issue of local law which will impact the outcome of these questions is the standard for record retention. Under Texas law, the Texas State Library and Archives Commission (TSLAC) is the agency that adopts records control schedules. The schedules are available on the Internet at www.tsl.state.tx.us. The current model records retention schedule for local governments promulgated by TSLAC does not address email. However, TSLAC has drafted a sample "Model Policy for Records Management Requirements for Electronic Mail." [7] Under Chapter 202 and the TPIA, a record that is the subject of litigation or a public information request may not be destroyed until the litigation is settled or the request is resolved.

In 2001, a Washington appeals court held that a series of emails between members of a school board constituted a meeting. In *Wood v. Battle Ground School Dist.*, 107 Wash.App. 550, 27 P.3d 1208, 155 Ed. Law Rep. 1437 (Wash.App., 2001) four out of five school board members sent each other email messages discussing whether a school district employee should be terminated. When the employee was later fired, she sued the school district for violations of Washington's Open Public Meetings Act.

The appeals court held that the exchange of emails can constitute a meeting if members communicate about issues that may or will come before the board for a vote. In doing so, however, the court recognized the need for balance between the right of the public to have its business conducted in the open, and the need for member of governing bodies to obtain information and communicate in order to function effectively. The opinion emphasized the fact that the mere use or passive receipt of email does not automatically constitute a meeting.

VII.
LITIGATION AND DISCOVERY
RULE 26 OBLIGATIONS

Fed.R.Civ.P. 26(a)(1)(B) requires a party to provide a "copy" of, or a description by category and location of, all documents, date compilations, and tangible things that are in the possession, custody, or control of the party and that the disclosing party may use to support its claim or defenses." More specifically, Rule 26(a)(1)(B) disclosures should "describe and categorize, to the extent identified during the initial investigation, the nature and location of potentially relevant documents and records, including *computerized data and other electronically-recorded information…*" "Computerized data and other electronically-recorded information includes, but is not limited to voice mail messages and files, back-up voice mail

[7] http:www.tsl.state.tx.us/slrm/recordspubs/lgbullb.html.

files, email messages and files, backup email files, deleted emails, data files, program files, backup and archival tapes, temporary files, system history files, web site information stored in textual, graphical or audio format, web site log files, cache files, cookies, and other electronically-recorded information." Furthermore, the disclosing party should take "reasonable steps to ensure that it discloses any back-up copies or files or archival tapes that will provide information about any 'deleted' electronic data."[8]

State Court discovery standards are either based on the Federal Model, or are very similar. They may have differences such as when the duty of production arises, but once it is triggered under the provisions of the rule, the outcome and obligation will be essentially the same. Litigators must focus on when the duty arises and who bears the burden of proof. That focus should be UP FRONT, and not after the ship has taken several rounds below the water line.

A common law duty to preserve information arises once there is a reasonable basis for anticipating litigation. Once a lawsuit is filed, that file or data retention obligation arises under the Rules of Civil Procedure.

As a general rule, that litigation hold does not apply to inaccessible backup tapes (e.g., those typically 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 (i.e., actively used for information retrieval), then such tapes *would* likely be subject to the litigation hold.[9]

Counsel must oversee compliance with the litigation hold, monitoring the party's efforts to retain and produce the relevant documents….to do this, counsel must become fully familiar with her the client's document retention policies, as well as the client's date retention architecture. This will invariably involve speaking with information technology personnel, who can explain system-wide backup procedures and the actual (as opposed to theoretical) implementation of the firm's recycling policy. It will also involve communicating with the "key players" in the litigation.

In short, it is *not* sufficient to notify all employees of a litigation hold and expect that the party will 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.[10]

The Court in the last episode of the *Zebulake* discovery dispute further noted that:

> "Counsel, in turn, failed to request retained information from one key employee and to give the litigation hold instructions to another. They also failed to adequately communicate with another employee about how she maintained her computer files. Counsel also failed to safeguard backup tapes

[8] *Super Film of America, Inc. v. UCB Films, Inc.*, 219 F.R.D. 649, 657 (D.Kansas)
[9] *Zubulake v. UBS Warburg LLC,* 220 F.R.D. 212, 218 (S.D.N.Y., 2003) (emphasis in original)
[10] L*aura Zubulake v. UBS Warburg LLC* Opinion and Order 02 Civ. 1243 (SAS) page 27

that might have contained some of the deleted emails, and which would have mitigated the damage done by UBS's destruction of those emails.[11]"

VIII.
SPOLIATION OF EVIDENCE AND SANCTIONS

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." The determination of an appropriate sanction for spoliation, if any, is confined to the sound discretion of the trial judge, and is assessed on a case-by-case basis." The authority to sanction litigants for spoliation arises jointly under the Federal Rules of Civil Procedure and the court's inherent powers.[12]

A Court sanction for spoliation can include costs, penalties, adverse rulings or the entry of default judgment, or a jury instruction allowing an adverse inference to be based on the destruction of evidence.

The spoliation of evidence germane "to proof of an issue at trial can support an inference that the evidence would have been unfavorable to the party responsible for its destruction." A party seeking an adverse inference instruction (or other sanctions) based on the spoliation of evidence must establish the following three elements:

1. That the party having control over the evidence had an obligation to preserve it at the time it was destroyed;
2. That the records were destroyed with a "culpable state of mind;" and
3. That the destroyed evidence was "relevant" to the party's claim or defense such that a reasonable trier of fact could find that it would support that claim or defense.

The Court in the *Zebulake* case awarded monetary sanctions in the form of deposition or "re-deposing" costs, and ruled that the following instruction would be give to the jury that hears this case:

> You have heard that UBS failed to produce some of the emails sent or received by UBS personnel in August and September, 2001. Plaintiff has argued that this evidence was in defendant's control and would have proven facts material to the matter in controversy.
>
> If you find that UBS could have produced this evidence, and that the evidence was within its control, and that the evidence would have been material in deciding facts in dispute in this case, you are permitted, but not required, to infer that the evidence would have been unfavorable to UBS.
>
> In deciding whether to draw this inference, you should consider whether the evidence not produced would merely have duplicated other evidence already before

[11] *Laura Zubulake v. UBS Warburg LLC*, 02 Civ. 1243 (SAS)
[12] *West v. Goodyear Tire & Rubber Co.*, 167 F.3d 776 (2nd Cir. 1999); *Fujitsu Ltd .v. Federal Express Corps.*, 247 F.3d 423 (2nd Cir. 2001); and *Kronisch v. United States*, 150 F.3d 112 (2nd Cir. 1998).

> you. You may also consider whether you are satisfied that UBS's failure to produce this information was reasonable. Again, any inference you decide to draw should be based on all of the facts and circumstances in this case.[13]

The Court made this philosophical observation and celluloid allusion:

The conduct of both counsel and client thus calls to mind the now-famous words of the prison captain in *Cool Hand Luke:* "What we've got here is a failure to communicate."

In the widely reported Phillip Morris case, the court imposed nearly $3,000,000 in sanctions as a penalty for email discovery defaults. The Court's opinion declines to enter judgment or give an adverse inference instruction, which the court seemed to think would be dispositive of the matter on the merits, and states:

> "There is no doubt that the Court has the authority to impose such a sanction for a discovery violation as serious and as irremediable as Philip Morris' destruction. *Webb v. District of Columbia*, 146 F.3d 964, 971 (D.C. Cir. 1998) *Shea v. Donohoe Construction Co.*, 795 F.2d 1071, 1074 (D.C. Cir. 1986). However, the Court has concluded, in the exercise of its discretion and with knowledge of the breadth of issues involved in this lawsuit, that such a far-reaching sanction is simply inappropriate.
>
> Second, the Government requests that Phillip Morris be precluded from calling Peter Lipowicz as a fact or expert witness at trial. That request is granted. Mr. Lipowicz, as well as any other individual who had failed to comply with Philip Morris' own internal document retention program, will be precluded from testifying in any capacity at trial.
>
> Consequently, Phillip Morris and Altria Group will be jointly required to pay a monetary sanction of $2,750,000 into the Court Registry no later that September 1, 2004. In addition, Phillip Morris and Altria Group will be required to reimburse the United States for the costs associated with a Fed. R. Civ. P. 30(b) (6) deposition on email destruction issues. Those costs are a minimal $5,027.48."[14]

In another recent case, the Baltimore Housing Authority found its ability to proceed at trial seriously impaired when sanctions were imposed after 80,000 emails were found and revealed, late in the game and after the close of discovery.

---

[13] This instruction was adapted from LEONARD B. SAND ET AL., MODERN FEDERAL JURY INSTRUCTIONS 75-7 (2004); *see also Zimmerman v. Associates First Capital Corp.*, 251 F.3d 376, 984 (2d Cir. 2001) (affirming district court's use of similar charge); *cf.* NEW YORK PATTERN JURY INSTRUCTIONS – CIVIL 1:77 (3d ed. 2004)

[14] *United States of America v. Philip Morris USA, Inc.* Civil Action No. 99-2496, Memorandum and Opinion

> "In this case, the Local Defendants were cautioned by the court that may objection to producing any the electronic records sought by the Plaintiffs would have to be particularized.
>
> A properly particularized showing of burden must be established by affidavit that identifies evidentiary facts to support the claims of unfair burden or expense.
>
> At trial, the Local Defendants will not be permitted to call as witnesses any former HABC/City personnel to testify with respect to subject matters that fall within the scope of any of Plaintiffs' Rules 34 requests that sought production of **email** communications, UNLESS the Local Defendants first demonstrate, by a preponderance of evidence, that (a) no responsive **email** communications were in the possession, custody or control of the Local Defendants *as of the date of the serving of the Rule 34 request*; or (b) that, if such documents did exist, they were produced to the Plaintiffs on or before April 1, 2003, or otherwise non-discoverable.
>
> Indeed, counsel for the Local Defendants herself was surprised, not to mention chagrined, by this **discovery**, having repeatedly told Plaintiffs and that court that **email** records either did not exist or already had been produced."[15]

Procedural issues are also critical. Several of the cases turn on the failure to properly preserve objections or to meet the burden of proof applicable under the rules. In re CI HOST, Inc., 92 S.W.3d 514 (Tex. 2002), the Texas Supreme Court initially refused to remedy an order to provide tapes which might have place the respondent in violation of Federal law. The Court noted, "CI Host offered no evidence to support its ECPA objection or any of its other objections at the hearing. The trial court overruled the objections and ordered production of the tapes." *Super Film of America, Inc.,* 219 F.R.D. 649, deals with another evidence failure context. The Court refused to allow a party to avoid discovery obligations to access its own data merely by claiming that it did not have the expertise to do so. "The Court finds SFA's conclusory contention that it does not have the expertise to retrieve such electronic data to be inadequate. Further, the court cannot relieve a party of its discovery obligations based simply on that party's unsupported assertion that such obligations are unduly burdensome." *Id. 657*

It is worth noting that a different litigation risk is presented by the phantom email conundrum, even if no sanctions or bad rulings come about. If you don't have it and know what it says, you can't evaluate your case, can't prepare your witnesses so that they don't fall off a cliff, and will end up behind the 8 ball. The other side will probably show up at trial with some errant copies that have been pirated within the organization, and make your whole team out to be a liar.

[15] *Thompson v. United States Department of Housing and Urban Development,* 219 F.R.D. 93 (D.Md., 2003)

IX.
COSTS

Short of crippling sanctions or instructions, there is the issue of the phenomenal costs that can be involved. Under the Federal Rules, the producing party generally bears the burden and costs of producing relevant and discoverable documents. The court may limit discovery if it determines that the burden of the discovery outweighs its likely benefit. Fed.R.Civ.P. 26(b)(2)(iii). To make this determination, the Court will consider what has been dubbed the proportionality test of Rules 26 (b)(2)(iii): the needs of the case, the amount in controversy, the resources of the parties, the importance of the issues at stake in the litigation, and the importance of the proposed discovery in resolving the issues. In this way, parties are protected from unduly burdensome or expensive discovery requests. Fed.R.Civ.P. 26(c).

See the interesting case of *Wiginton v. CB Richard Ellis, Inc.*, 2004 WL 1895122 (N.D.Ill.), which provides a window into the process and cost of evaluating a large, multi-location data system in a class action case, with a discovery project originally priced at $61,000 which mushroomed to $249,000 and was still full of holes.

See also *Zubulake v. UBS Warburg LLC.*, 217 F.R.D. 309 (S.D.N.Y. 2003) (Zubulake I) (addressing the legal standards for determining the cost allocation for producing emails contained on backup tapes); *Thompson v. Usdhud* 220 F.3d 241 (4th Cir. 2000); *Hagemeyer North America v. Gateway Data Services Corp.* 2004 WL 1810273 (E.D. Wis.)

X.
RISK MANAGEMENT

It is now necessary for lawyers advising their clients or carrying out discovery obligations to learn what is possible with the particular systems of memory storage, communication and retrieval. Simple initial inquiry is not enough. A generic understanding of the electronic data storage capabilities is also not enough. Waiting for others to carry the ball can be a mistake as the lawyers in these other cases have learned.

The particular system specifications and configurations, as well as the computer security back up and retrieval specs for the multiple systems must be evaluated. This includes evaluation of individual work stations as well as the larger network servers or other systems. It may require inquiry and evaluation of external host servers, either as a part of a particular entity's I.T. system, or *ad hoc* where email has been sent to others, and subsequently lost or deleted. Someone must determine who has set up different tools or techniques for the legitimate and efficient operation their own work program, or who has learned how to circumvent or manipulate the system.

Carrying out these responsibilities requires an understanding of how recovery is routinely accomplished, and what special technique tools and technicians may be able to accomplish. A simple inquiry about the existence or availability of back-up tapes may not be sufficient. Back-up tapes or drives may sometimes be restored in original or partial data recovery accomplished.

The different compartments within which the city attorney must function to meet this new set of responsibilities include:

1. Participating in the development, implementation, and enforcement of city wide email policies
2. Evaluating the truth and accuracy of claims by opposing interests (litigants, vendors, potential or existing contract, partners etc.) and understanding of the system specifications and document retention architecture;
3. Participating in the development of a culture which does not create and even amplify the necessary evidence to support city liability in a myriad of contexts including sexual harassment, negligence, discrimination, retaliation, and so forth;
4. Participating in the development of a knowledgeable and sophisticated litigation discovery system which serves the city's interest well when its adversaries possess and use electronic information.
5. Participating in and supervising defense litigation practices to ensure that the city is in compliance with its legal obligations under the law for identification and production of electronic information in accordance with the law, and thereby avoid the potential imposition of sanctions, or adverse rulings on the merits.

Without a comprehensive understanding (yours or your consultant's) you may be able to determine that something no longer exists, or that part of it is gone or missing, but fail to understand how the absence or trail of disappearance actually proves contested or controverted facts. See for instance the discussions in the *Zebulake* case about the clues and references to missing email, and the chronological significance of that evidence when overlaid with the testimony of the witnesses. [16]

A strategic decision should be made about the effectiveness of a policy, and then a strategic decision must be made about triggering and announcing a compliance phase. There will be pros and cons of taking the quiet approach verses the noisy approach. Each of those options and considerations need to be taken into account. Nevertheless, the step needs to be taken to make sure that everyone knows what the policy is, that it will be enforced, and what the enforcement options will mean to them. Just like a random drug testing policy may change choices, the knowledge that individual computer work stations will be randomly selected for compliance auditing this next weekend will have an effect. Once the choices have been made and the notification had been given, in order to resolve privacy concerns, an initiative for management enforcement and for random auditing should be implemented immediately. No policy will ever work without these steps. The organization will remain vulnerable to liabilities in their absence. Individual employees will remain vulnerable to their own tendencies for poor choices, which will result in on-the-job inefficiencies, and may result in susceptibility to termination, or even criminal prosecution. Carrying out these programs effectively allows everyone to seize the day, go through rehab, achieve email and internet redemption, and improve the work place.

[16] Davies testified that he was unaware of Zublake's EEOC charge when he spoke with Orgill. The timing of his emails, however – the newly produced email that acknowledges receiving Zubulake's EEOC charge coming three hours before the email beginning "I spoke to Brad" – strongly undercuts this claim. *Id. 19*.

XI.
WHAT YOU SHOULD DO AND WHEN YOU SHOULD DO IT

1. Meet with the City Manger, Mayor or other chief executive officer immediately. Explain the high level of vulnerability that exists, and obtain authorization to be a proactive participant in a team to establish an appropriate policy and program for enforcement;
2. Have an immediate meeting with I.T. staff personnel. Make sure to discuss, consider, and include the official email internet tools, as well as all of the other individualized and personal details and interfaces;
3. Conduct a system inventory for your own understanding of the issues;
4. Having taken these steps, participate with your chief executive to choose and select a designated team. Either include yourself on that team as the city's lead lawyer, or designate a trusted subordinate or colleague to carry out that role. Start this team on policy evaluation.
5. Obtain a joint commitment throughout the management team with the assistance of your I.T. group. This will require a clear message from the top, and an understanding for each department or division of its level of priority, and the full intention to enforce and apply it.
6. Develop a fair, appropriate and nondiscriminatory auditing approach to assure compliance.
7. Make sure that your system and policy is based upon an accurate understanding of the parameters of the attorney client privilege, and that every step is made to preserve the privilege on behalf of those who are appropriately a part of that relationship.
8. Require that your formalized litigation management system, program, or documentation include specific planning and evaluation by responsible counsel on the subject of electronic information and its discovery, and that case management oversight is routinely directed to that subject in order to habitualize.