LooperReed & McGraw ATTORNEYS

Document Retention: The 800 lb. Gorilla

BY

MICHAEL KELSHEIMER

EMPLOYMENT SECTION – LOOPER REED & MCGRAW, P.C.

JASON RODRIGUEZ

IT MANAGER – LOOPER REED & MCGRAW, P.C.

This booklet is for informational purposes only and should not be considered legal advice. Additionally, the concepts addressed in this book are meant as general guidance only; specific legal issues should be discussed with qualified legal counsel.

TABLE OF CONTENTS

Document retention is a matter of growing importance for both lawyers and clients. I often characterize it as the 800 lb gorilla in the corner of the room that no one wants to talk about. Lawyers and clients perceive document retention as time-consuming, troublesome, and most importantly, difficult to understand. Not because the subject itself is too complex, but because it involves computers and servers which are as much a mystery to most people as the inner-workings of their car.

Many litigators even refuse to push for electronic documents from opposing parties because they have not adequately prepared their client for the inevitable reprisal. To make matters worse – most clients simply don't have the time or resources to devote to a litigation hold when potential disputes arise. They all know the gorilla is there watching, waiting, staring, and that it will someday come out of the corner and clobber them. For today, however, everyone feels there are more pressing problems to address.

One thing is certain. If you wait until you receive that first request from opposing counsel when the information really matters, you won't even hear the gorilla coming . . .

I've done my best to make the subject workable by breaking it down into three basic categories: Avoiding Bad Data, Creating Document Retention Policies, and Instituting Litigation Holds. From there, each subject is further divided into smaller steps that hopefully make the topic seem digestible, if not smooth, going down.[1],[2]

AVOIDING BAD DATA

Garbage in – leads to – garbage out. It won't matter that you have the most sophisticated document retention policy in the world if relevant, producible, information destroys your case. The most common source of garbage data is poorly thought-out email. If mom was right when she advised us to think before we speak, she certainly would have been right in advising us to think before *writing* an email. Emails often sit on servers months or years waiting to rear their ugly head when a request for production comes in.

I don't know if the following examples are all real emails, but they perfectly illustrate the potential damage emails can cause:

> *Client to In-House Counsel:* "I think this is illegal, but I'm going to do it anyway, unless you tell me not to."

[1] This guide is not designed to be "read" as though it were an article. Instead, it is a practical tool to help you work through the process of dealing with document retention from start to finish. Reading it like an article could result in that overwhelming sense of despair that most people feel when thinking of document retention (even though this is an exceptionally distilled version of the thousands of pages of data and cases I have sifted through to prepare it). Use it accordingly, and remember the advice mom used to give . . . How do you eat an elephant (or in this case a gorilla)? One bite at a time!

[2] If you run a Fortune 1000® company or a multi-national conglomerate, this guide will fall far short of all of the considerations needed for a business of your size. It might serve to give ideas, but should not be the sole basis for dealing with document retention. If your business\client is this large – congratulations, and give me a call for more detailed advice suited to your circumstances.

Client to Client: "We could do [blank] and we would probably go into the fiery pits of hell. ha. ha."

Between Microsoft Execs: "I personally got burned by the Intel 915 chipset issue . . . I chose my laptop because it had the vista logo and was pretty disappointed that it wouldn't run Glass, but more importantly, it wouldn't run Movie Maker. I now have a $2100 email machine."

Between Microsoft Execs: "In the end, we lowered our requirement to help Intel make their quarterly earnings . . ."

Between Credit Rating Managers: The agencies are creating an "even bigger monster – the CDO market. Let's hope we are all wealthy and retired by the time this house of cards falters."

Between Client Managers: "We are in breach of this agreement and need to discuss."

Email has moved far beyond the tool it was originally designed to be. It has morphed into a form of on-going conversation that has lost its formality. This is especially true because we are often more bold in writing than in person. For these reasons, it is important that you regularly remind every member of your staff of the danger posed by writing things in emails that would cause them apoplexy if discovered in an agreement or other documents sent to a recipient outside the company.

Follow these steps to improve the quality of your company's email:

Step 1: Implement a personal email policy. Personal emails, much like personal calls, are impossible to totally root out of your system. Unless you run a Stalinistic workplace, it is unrealistic to expect that you can maintain a pleasant work environment without your staff sending personal emails. For that reason, I recommend your staff use third-party, internet-based, email accounts such as Gmail®, Hotmail®, or Yahoo® for their personal communication. If they use an internet-based system, the communication won't be stored on your server or realistically subject to discovery.

Step 2: Give pointers. Present your staff the following top ten list for writing emails:

10. Get to the point right away.

9. Proof-read.

8. No potty mouth.

7. No criticism about co-workers.

6. Avoid being too informal.

5. Think about the value of a face-to-face conversation vs. sending an email. Some companies have even implemented no-email Fridays.

4. Remember – sending a letter from your work account (which lists the business name in the address) is a reflection on the company.

3. Scrub (remove the metadata) any file you attach to an email that is going outside the company.

2. Be careful with reply to ALL.

1. Follow Mom's advice: Think before you . . . write.

Make these pointers part of your staff handbook, and as much as it will pain you, *enforce* them. It is human nature, not just that of children, to heed warnings only when they count for something. If your staff learns that you won't enforce these rules, they, and you too, will eventually fall back into bad habits.

Step 3: Implement restrictions. Consider implementing rules restricting staff members from communicating about work topics via instant message or, the latest rage, Twitter. Case law is just now starting to provide serious guidance for e-discovery, so there certainly are not cases talking about whether instant messages are something that must be saved. If it is relevant, however, you can bet that there will be case law on it in the future and you don't want to be the test case. By implementing a policy against using these mechanisms for work communication, you decrease the risk that you will become responsible for retaining such information.

See, this is not so hard. Now, let's move on to creating a document retention policy.

CREATING DOCUMENT RETENTION POLICY

I begin this section by introducing a concept that I will use often – If you couldn't explain it to a judge with a straight face, don't do it. In creating your document retention policy and instituting litigation holds you will be tempted to institute rules that might be questionable. Don't succumb. When reviewing the case law, I observed that courts treat e-discovery with a lot of common sense. If your policy was thought out and reasonable, you are likely to avoid sanctions, potentially significant expense, and the death knell that a spoliation instruction would sound for your case.

It is not required that you have a document retention policy. Let me repeat, you don't have to have one if you don't want to. That said, the benefits of document retention are simple to understand: organization of information, increased storage space, and for our purposes –

making litigation holds easier to implement. Without a document retention policy, trying to preserve data once a dispute arises will be much more difficult, though it can be done.

The overarching theme in cases regarding document retention policies is reasonableness. Yes, the "reasonable man" lawyers feared in their law school torts class is back. If your policy is reasonable, you will likely avoid the wrath of a judge. What is reasonable, though? Without going through each case, let me simply say that you can avoid potential difficulties with a court by following the advice above – don't do it unless you believe you can explain it to a judge with a straight face.

Some of you might ask, "What about all of the cases where people are sanctioned for e-discovery violations?" With a few exceptions, noted below, court decisions about data retention don't generally involve document retention policies. Rather, they concern litigation holds that halt the process of document elimination.

There are four basic steps to take when creating a document retention policy: Identify, Evaluate, Implement, and Enforce.

Step 1: Identify. Before you can decide what your policy will be, you've got to take a look at the rules and other factors that affect how it will look:

⇒ Whether you are aware of it or not, many federal and state laws require retention of certain documents, thus affecting every business' document retention policy. A partial list of federal laws is included at the end of this guide. I learn about new requirements all of the time, so you cannot count on this list to be complete. Examine the laws that affect your business and list each of the requirements that affect you.

⇒ The electronic storage systems used by businesses vary incredibly. Trying to take into consideration each permutation and its impact on the way you build a document retention policy is far beyond the scope of any guide on document retention. What I can offer you is a basic list of places where you may find information stored:

- Home computers[3]
- Laptops
- Desktops
- Servers
- Back-up tapes[4]
- Cd-Roms
- Flash drives[6]
- GPS\Black boxes
- Audio recordings and voicemail[7]
- Instant messages[8]

[3] *Orrell v. Motercarparts of America*, 2007 WL 4287750 (W.D.N.C. 2007)
[4] Some courts say, "No." Others say, "Yes:" *Zubulake v. UBS Warburg LLC*, 220 F.R.D. 212 (S.D.N.Y. 2003) (Back-up tapes generally inaccessible data and not required to be preserved); *Treppel v. Biovail Corp.*, 249 F.R.D. 111 (S.D.N.Y. 2008) (saving required).

- Cell phone pictures[5]
- PDAs

You will need to take the types of information you use into consideration in molding your policy.

⇒ Not only do you have to consider the electronic data you possess, but the software which makes that information accessible. Do you have custom-designed software? What happens if you change software? Will the data in the old program be fully available in the new program? If, for example, you abandon Microsoft Outlook® to move to a new system, you must be able to get to the old information when it becomes relevant in discovery. Take this into consideration when switching programs and be certain to maintain licenses until all the documents which utilize the old software have been deleted under your document retention policy.

⇒ While making sure you keep old software, you also must make sure to keep hardware to access the information. After all, how many of you have seen a 5.25" floppy drive lately?

⇒ Though this guide focuses on electronic information management, you must give similar consideration to paper data. The following examples offer a starting place in considering sources of paper data which might not also be kept electronically:

- Signed documents
- Handwritten notes
- Calendars
- Accounting\tax records
- Bills\statements from vendors
- Correspondence
- Memos
- Plans\drawings
- Company policies
- Deeds\leases
- HR files
- Requests for proposal
- Marketing materials and presentations
- Billables\payables records
- Building plans\drawings
- Photographs

[6] *Columbia Pictures Industry v. Bunnell*, 2007 WL 2080419 (C.D. Cal. 2007)
[7] *E*Trade Securities LLC v. Deutsche Bank AG*, 230 F.R.D. 582, (D.Minn., 2005); *Del Campo v. Kennedy*, 2006 WL 2586633 (N.D.Cal. 2006)(unpublished opinion).
[8] No cases directly on point at this time.
[5] *Smith v. Café Asia*, 246 F.R.D. 19 (D.D.C. 2007)

⇒ Many companies outsource one or more functions of their business. These outside documents must also be considered because they are within your "control" for discovery purposes.

What you control is broader than what you possess. You may not possess your accountant's file for last year's taxes, but you do have control over it. Not only must you consider what your document retention policy will be for this type of information, you must also consider your vendors' document retention policy. If they would otherwise eliminate your data in a period that is different than you prefer, it can adversely affect you. Imagine if you produced thousands upon thousands of pages of documents for a lawsuit that is now over. The data has been deleted at your office, but your law firm has a 5-year retention policy or no policy at all. The documents you provided the law firm are within your control and include information that you otherwise have long since forgotten. This information may be discoverable in subsequent litigation. You must account for it in your document retention policy.

⇒ Some businesses have rules regarding document retention in their by-laws or other organizational documents. Make sure that you take these rules into consideration when determining your policy. You will not be able to explain with a straight face that you deleted documents under a document retention policy which is inconsistent with your own corporate by-laws or regulations.

Step 2: Evaluate. Now that you have outlined all of the rules and other parameters that will affect your document retention policy, you can begin to formulate the framework for the policy. The factors identified here cannot be considered exclusive or exhaustive because each business is different and will have different goals and needs. The following will, however, serve as a solid base upon which to build your plan:

⇒ The simplest, most effective, document retention policies are *very restrictive* on the rights of users regarding where and how data is stored. For this reason, it is important to consider the psychological aspects of the policy you create. Executives and senior management may find such a policy too restrictive, preferring to take risks rather than deal with the infringement on their freedom and control over data. You may as well deal with it up front.

⇒ There are software solutions to assist with document retention. These programs range from relatively inexpensive to very expensive customized document management systems, or "DMS." Regardless of whether you utilize a DMS, preparing a document retention policy will largely be influenced by the software you use.

⇒ In creating the plan, you will also need to consider the questions below. Again, this list is not exclusive because I don't know your individual business needs, management style, or computer system. Nonetheless, it serves as a great starting point:

- What will you do when a staff member leaves? Will the computer hard drive be kept for a period of time in case there is needed information or the staff member attacks the company for discrimination or unemployment income?

- How long will you keep each category of paper documents that you identified during Step 1?

- How long will you keep each category of electronic documents that you identified during Step 1? Be wary of especially short retention periods. Businesses that try to avoid bad data by implementing very short document retention policies may have trouble explaining to a judge with a straight face the business purpose for the shortened policy.[9]

- How will records be destroyed? Will paper documents be shredded? Will electronic documents be deleted utilizing an automated system, or will there be a person responsible? If an individual is responsible, what process will be in place to remind them?

- As they pass the end of their retention period, when will data be destroyed – Weekly? Monthly? Yearly?

- Who will be responsible for: (1) destroying data; (2) enforcing the policy; (3) re-evaluating the policy when changes occur; (4) recognizing the need to suspend the policy in the face of possible litigation, a subpoena, or governmental inquiry; (5) managing data held by outside sources, such as law firms and auditors; and (6) assigning new people to manage the policy when others move on to new positions or leave the company?

- When will the policy be suspended? What will the process be for: (1) litigation holds; (2) governmental inquiries; and (3) subpoenas?

- What will be the procedure for various hold types? Clearly lay out the process to be followed in each instance.

- How will you document the destruction of data according to the policy? You will want to be able to show a court or governmental agency that you have systematically followed the policy.

- How will you organize documents moving forward from the time the policy is implemented? Will you use naming conventions? What will your file structure look like? Will you mandate storage in specific locations? Will you restrict the use of certain storage devices? The structure for every business will be different because of the software applications, management style, and other unique characteristics of the business.

[9] *Broccoli v. EchoStar Comm.'s Corp.*, 229 F.R.D. 506 (D. Md. 2006) (two week retention policy for email questioned).

- How will you deal with data that exists at the time the policy is implemented? Paper documents can be sorted and deleted based on the schedule. Electronic documents may be difficult, if not impossible, to organize into the file structure you implement for new data, thus requiring a different plan. As you will see below, I recommend that you do not attempt to restructure old data.

- What is your present back-up system and how will it impact your document retention policy? Back-up plans are entirely different than document retention policies, though the two overlap concerning the *accessibility* of information. Though there are many forms of back-up they range from easily accessible systems to very difficult to utilize for purposes of obtaining old information. The more difficult information to access has been characterized as "inaccessible" by some courts.[10] There is a debate about whether "inaccessible" back-up information must be kept during a litigation hold. You may want to seek the advice of an attorney on this point in the event litigation arises.[11]

- Is it appropriate to move toward a paperless office by scanning all documents? This process will reduce the physical storage space your business requires and make it easier to implement a hold because there will be little paper data to sift through.

- What will your policy be with respect to instant messaging, Twitter®, and cell phone photography? Will you instruct staff members not to use these devices for work purposes? If you allow them for work purposes, how will you collect and store them in the event the policy is suspended for a hold? Similarly, will you instruct staff they may not use company-provided computers, phones, and other devices for person communication?

- What will be the penalties for failing to comply with the policy? You have to enforce the policy for it to have value. A policy with no teeth will not be followed.

- What is the interval at which you will reconsider and reevaluate the policy because of changes in your staff, workplace, computer system, or laws affecting the business?

- How will your staff let you know they believe the policy needs to be suspended for a hold based upon information they possess or a situation they encounter?

Step 3: Implement. The following represents *an approach* to document retention that can be used on almost any server-based computer system. Elements of this plan may or may

[10] Note, some companies do not have separate disaster recovery tapes and only have "accessible" back-up tapes. If this is the case, there will not be a separate need to keep disaster recovery tapes because there are none!
[11] *Zubulake v. UBS Warburg LLC*, 220 F.R.D. 212, 218 (S.D.N.Y.2003) ("inaccessible data" not required to be kept); *but see Treppel v. Biovail Corp.*, 249 F.R.D. 111 (S.D.N.Y. 2008).

not work for you, but you can certainly use it as a jumping off point for what will become the policy that is unique to your business: [12]

⇒ Old Data. This is paper and electronic data that exists in your business now – before the policy is implemented. Because it would consume amazing amounts of time to attempt to reorganize your existing data into the format of your new policy, it is not practical to ask you to do so. Begin by eliminating everything you presently hold that is older than the cut-offs set in the new policy. Then, going forward, delete the old information according to the policy. During this transition period, make sure to keep a license for any old software programs and hardware (remember that old 5.25" floppy drive) that are used with old data.

⇒ New Data. Remember, the legal purpose for having a document retention policy is to make it easier to institute a litigation hold when it becomes necessary. Highly organized and centralized file systems are the easiest retrieve data. If you put all of your data in one computerized "filing cabinet" (your server) and implement strict rules regarding the place new data will be stored in that cabinet, there is only one place you have to go when it comes time to find the data for a hold. Hence, I recommend a two-pronged approach for electronic data on a going forward basis:

- Email. It is unwieldy and difficult to manage, especially on a computer system where users have their own laptop or desktop. The biggest problems with email are: (1) staff deleting them; (2) organizing them; and (3) personal communications. Even if you have a centralized email system, your staff generally can delete emails from the system *permanently* at their desk. In this type of system, each staff member also chooses how to organize and store emails that are kept for future reference or use. Short of implementing a document management system, there are relatively few things that can be done to control staff behavior with email which they cannot circumvent. Nonetheless, you should implement the following three practices:

  - Require staff to use third-party, internet-based, email systems for personal communication. Preventing staff from sending personal emails is almost impossible. Acknowledging the futility of trying to stop personal emails, I suggest allowing staff to access third-party, internet-based, email systems such as Gmail®, Hotmail®, or Yahoo®. Requiring their use will allow you to keep personal emails off your server and the added benefit of reducing the storage space for retained data.

[12] In preparation of this guide, I spent many long hours with our in-house IT Manager, Jason Rodriguez (a man with more certification initials after his name than any person should have). While discussing implementation of a document retention policy from an IT perspective, we considered the simplest conceivable policy, given our lack of knowledge regarding your computer systems. You will need to tailor a plan based on your system, but we have done the very best we can to provide basics which will be applicable to any server-based system.

- Restrict your staff's ability to permanently delete email. Though there is no means to accomplish this electronically unless you utilize a special system, make it part of the requirements your staff must follow. Also, your IT Professionals need to restrict your staff's ability to archive email. This will allow *you* ultimate control over deleting email.

- Require your staff to use "naming conventions" for saved email. Naming conventions are a system by which everyone uses the same name for a folder in which they store emails related to certain subjects. For example, if you have a client named George Carlin, each staff member would create a sub-folder called "Carlin" in their email folder and save all emails related to Carlin in that sub-folder. By using this system, the data related to each subject will be uniformly stored in sub-folders in each staff member's in-box.

- Similarly then, you can create "naming conventions" for the subject line of emails. For emails related to Carlin, staff members must put Carlin in the subject line somehow. It could be as simple as "Carlin: Is the Request for Proposal ready?" This will help you find emails if you have to search the system.

o Other Documents. Virtually all other documents will fall into the remaining category which includes word processing files, spreadsheets, plans, memos, notes, calendars, etc. While not as unwieldy as email, these documents are also difficult to control. With the amazing variety of media available to save data, the goal is to force all data into the single "filing cabinet" discussed above. To accomplish this, you will need to:

- Instruct staff to save all documents to the server. Temporary copies made for working remotely; transferring data via flash drive, CD Rom, or other media; or on laptops, must be deleted after use. No drafts or other documents will be kept on any source other than the server. This isn't to say that your staff must refrain from ever copying data off the server, but that the data must be removed from the alternate source when its usefulness is complete. Also instruct your IT Professional to disable or severely restrict the staff's ability to save documents "locally" or on their "C:\Drive." If you cannot do this, have your IT Professional regularly delete this data from each individual computer.

- Implement the same naming convention utilized with email for the storage of documents. Create one, and only one, location on the server for files to be stored related to a single client or project such as "Carlin" in the examples above.

- Implement a policy of deleting all voicemails after a certain period of time because they are discoverable.

- Implement negative policies. Instruct your IT Professionals to restrict access to instant message programs and websites like Twitter®. If you cannot do this, instruct your staff that instant messaging, Twitter®, and the like, may not be used for work purposes. Prohibit recording conversations by staff members unless it is part of your business.

⇒ Achieve Buy-in. Without it, the whole process will be lost from the start. People do a much better job of following instructions when they understand *why* it is important.

- It is absolutely imperative that your IT Professionals understand why data must be deleted in accordance with the policy. IT Professionals don't like to get in trouble and that often occurs when data is lost. For this reason, they are very often data pack-rats. Stories abound of IT Professionals saving data in odd places, including their home garage, because they are afraid it may be needed some day. You must make them comfortable with the policy.

- Your staff, too, should understand the policy. Make it part of your staff handbook.

Step 4: Enforce. There is no sense in having a policy if you do not enforce it. As a matter of fact, the opposite is true. If you have a policy and do not enforce it, you will not be able to explain it to a court in a way that excuses your failure to follow it. If data is missing that should otherwise be available under your policy, it will not go well for you with a court.

⇒ Follow the penalties you set out in the policy.

⇒ Remember to consider the policy when things change in your business. For example, if you switch email systems don't forget to review and implement appropriate changes to the policy. If your IT Professional or someone else responsible under the policy leaves the company, appoint a replacement and get them up to speed.

⇒ Review the policy at the intervals set out in it.

INSTITUTING LITIGATION HOLDS

An attorney asked me, "What is the simplest advice I can offer a client regarding document retention, and more particularly litigation holds?" I replied, "Save everything." If you save everything, your only concern is the cost of locating and producing the relevant data. While these costs could prove enormous, you will never find yourself facing sanctions or an instruction to the jury that there was data missing, which they should presume was negative to your position. It is also the only answer I can offer without getting into the specifics of instituting a litigation hold.

I respect this query because the vast majority of small\medium sized business owners don't even have a staff handbook (I encounter it all the time in my practice). Why would they take a step further and have a document retention policy?

The attorney above scoffed at the idea of saving everything because it was "totally unrealistic" to expect the business owner to do so. Unfortunately, it is a quandary without a good answer. Certainly, an intelligent business owner, without a legal background, could try to make the right decisions about saving information once learning a dispute was possible. They might even escape the wrath of a judge, but, in the end, the only way to be certain is to follow the advice below or save everything and bear the cost.

Litigation holds are the single most challenging, time consuming, and important aspect of document retention. Nonetheless, I've broken it down into pieces that should be relatively easy to follow. It begins with the trickiest part of implementing a litigation hold – knowing when the obligation starts. Get it right, and there are no problems. Get it wrong, and you could find yourself facing sanctions, or worse, from a judge who doesn't believe that you chose the right occasion to start holding data.

The simplest way I can explain it is that the obligation arises when a "reasonable person" (not necessarily your business owner) would anticipate litigation.[13] Yes, to lawyers this sounds a lot like the point at which the work-product privilege attaches, but to clients, it often is not clear. For example, in my area of experience, the question arises when the obligation to retain data begins in discrimination disputes. Does it begin when the staff member makes a complaint of discrimination, while still employed with the company, and long before termination or quitting? Is it when the staff member refuses to accept a severance package that requires signing a release of liability after separation? Does it attach later when a discoverable email is sent between two staff members confiding that they suspect the former staff member will sue? Or, is it later, when the EEOC request for information arrives? [14] This is hard for lawyers to answer, much less a business owner.

Every court's interpretation on this point may be different, so there are two pieces of advice I can offer to protect you or your client: (1) start early – you can always stop the hold later; and (2) document your reasons for starting when you do. This comes back to the idea of saying it to a judge with a straight face. If you have a rational, intelligent reason for starting the hold at a particular point, you are likely to avoid negative consequences.

The starting point defined, what then is the scope of your obligation? How much information should you keep? You could go with the "save everything" approach and stop reading right here …. Tempting isn't it? Unfortunately, as I mentioned above, there is one big

[13] In Texas courts, the duty to preserve evidence does not arise until a party knows or reasonably should know that there is a substantial chance a claim will be filed, and such evidence is relevant and material. *Wal-Mart Stores, Inc. v. Johnson*, 106 S.W.3d 718, 722 (Tex. 2003). In federal courts it is virtually the same, the obligation to preserve evidence 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." *Fujitsu Ltd. v. Federal Express Corp.*, 247 F.3d 423, 436 (2d Cir. 2001). Thus, "[o]nce 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 v. UBS Warburg LLC*, 220 F.R.D. 212, 218 (S.D.N.Y. 2003).

[14] *Id.*

reason you might not want to follow this approach – the cost of keeping everything can be enormous. In case you were unaware, back-up tapes are expensive. Our firm uses six tapes every week for back-up at a cost of about $150 each. If the firm could not recycle the tapes each week, the cost would become astronomical in a short period.

To truly save everything, you would not be able to delete any of these tapes. Why, you might ask, can't I just save the last tape of the week or at the end of each month? The answer is simple. It won't retain previous versions of documents. For example, you edit a word-processing document on Tuesday and it is backed-up that night. On Friday, you change it again and that night it is again backed-up. Unless you keep the Tuesday tape, you won't have the previous version of that document. Sorry. It is a pain, but that is the way it is.

Since you are still reading, I'll assume you don't want to save everything. The scope of your obligation is then governed by state and federal rules of procedure,[15] but includes documents within your control:

⇒ Known to be relevant;

⇒ Reasonably should be known are relevant;

⇒ Reasonably calculated to lead to the discovery of relevant evidence;

⇒ Reasonably expected to be requested; and

⇒ Subject to an existing request.

So what happens if you get it wrong? You will get to learn the meaning of spoliation. Spoliation is the legal term for the destruction of evidence relevant to a case.[16] It does not have to be intentional for you to be subject to sanctions.[17] In Texas, the burden is on the party claiming spoliation to prove the "spoliator" failed to preserve discoverable evidence.[18] Once spoliation is determined, courts must fashion an appropriate remedy by considering several factors.[19] The penalty, in both state and federal court, is within the discretion of the trial court, difficult to overturn on appeal, and can range from monetary sanctions to an instruction to the jury that the missing evidence was destroyed in bad faith because it would have reflected negatively on the spoliator.[20],[21] When issued, such an instruction often forces a settlement of the case because of the difficulty in overcoming the idea it puts in the jurors' minds.[22]

---

[15] Fed. R. Civ. P. 26(b); Tex. R. Civ. P. 192.3; see also *Zubulake v. UBS Warburg LLC,* 220 F.R.D. 212, 216 (S.D.N.Y.2003); *National Ass'n of Radiation Survivors v. Turnage,* 115 F.R.D. 543, 556-57 (N.D.Cal. 1987).

[16] *Buckeye Retirement Co. v. Bank of America, N.A.*, 239 S.W.3d 394, 401 (Tex.App.-Dallas 2007, no pet.).

[17] *Wal-Mart Stores, Inc. v. Johnson*, 106 S.W.3d 718, 721-22 (Tex.2003).

[18] *Id.*

[19] When considering an appropriate remedy for spoliation, a trial court must determine (1) whether there was a duty to preserve evidence, (2) whether the alleged spoliator negligently or intentionally spoliated evidence, and (3) whether the spoliation prejudiced the opposing party's ability to present its case. *Buckeye Retirement Co.*, 239 S.W.3d at 401 (citing *Trevino v. Ortega*, 969 S.W.2d 950, 954-55 (Tex.1998)).

[20] *Wal-Mart*, 106 S.W.3d at 723; *McMillin v. State Farm Lloyds*, 180 S.W.3d 183, 199 (Tex.App.-Austin 2005, pet. denied); *Whitt v. Stephens County*, 529 F.3d 278, 284 (5th Cir. 2008).

Sometimes the penalty can even be levied against the lawyers involved and not the client.[23] It has become the lawyers' responsibility to make sure that their clients do, in fact, retain all of the available information. To be sure you heard – lawyers are responsible and can be individually sanctioned for failing to make their clients retain documents. With this final warning, you may begin the process of instituting a hold.

The following five steps will carry you from start to finish: Investigate, Collect, Follow-up, Make a Deal, and Utilize\Produce.

Step 1: Investigate. At the beginning of the process you need to learn what happened, especially if you are not directly involved in the dispute from which the hold arises. During the time you are conducting your investigation, you need to make sure that relevant data is not lost. Notify your IT Professionals and other staff to cease deleting ALL data, and to preserve existing data in pristine form, including things such as the hard drive from the computer used by a staff member who is suing.[24] Remember, deleted information on a hard drive is not really gone until it is saved over with new data, so continuing to use the computer risks loss of that pseudo-deleted data. You also need to warn potential outside sources of data, such as accountants, attorneys, or payroll companies about the need to avoid deleting information during the investigation.

Next, you must put yourself in the shoes of opposing counsel. Think of yourself as Columbo or Matlock. What information would you want to help you prove your case? It is important to be realistic at this point. If you marginalize the opponent's position in your mind, it will likely cut back on the information you preserve, putting you in the position of possibly running afoul of a judge. At this stage you should err on the side of saving too much information rather than too little. Make notes of this investigation in case you are ever called upon to justify your choices.

From there, outline: (1) Who – is involved or has data; (2) What – data is available and relevant; (3) Why – has the dispute arisen and what documents are involved, (4) When – did the dispute arise and how far do you have to go back to preserve the relevant data, and (5) Where – is the data located electronically and physically.

This should be followed by interviews of all of the key players connected to the potential claim. Take their deposition, so to speak. This will help you identify the documents which

---

[21] Spoliation instruction only available for bad faith destruction. *Condrey v. SunTrust Bank of Ga.*, 431 F.3d 191, 203 (5th Cir.2003). Typically an inference of bad faith is not allowed when documents are destroyed under a routine policy. *Vick v. Tex. Employment Comm'n*, 514 F.2d 734, 737 (5th Cir.1975); see also *Coates v. Johnson & Johnson*, 756 F.2d 524, 551 (7th Cir.1985) (declining to make inference of bad faith when documents were destroyed according to routine procedures).

[22] *Zubulake v. UBS Warburg LLC*, 220 F.R.D. 212, 219-20 (S.D.N.Y., 2003).

[23] *Zubulake v. UBS Warburg LLC*, 229 F.R.D. 422 (S.D.N.Y., 2004) was the first major case to put the idea of attorney responsibility into the fore of e-discovery considerations. Others have since followed.

[24] Every day you use a computer that has relevant information on it, you increase the risk of losing data. You ask – "Why does that happen if I don't delete anything?" The reason is this: Data you previously "deleted" may still be on the computer. When you press "delete" the computer does not scrub that data off the hard drive. It just goes to the beginning of the section where the data is saved and places a "0" so that the next time the computer needs to store new data, the old data may be written over. Until new data takes its place, the old "deleted" data is still accessible by someone with the right forensic computer skills.

need to be held and provide a better understanding of the claim when litigation starts. Ask who the other key and tangential players are (remember they will be asked this question in deposition). A judge will not like it if you utilize only the list *you* created to decide whose information to keep – especially if a key player later identifies someone else in deposition. Also ask what the key players perceive to be the key and tangential documents (electronic and paper), where they are located, and how have they been stored. It is appropriate to go over the list of paper and electronic document types outlined above as a primer, to identify all of the relevant sources of data.[25] And, don't forget drafts of documents.[26]

Discuss outside sources of data that may be relevant. Documents in the hands of auditors, accountants, payroll companies, lawyers, or others are within your control and therefore must be kept. If the outside source is unaware, it may delete your documents under its own retention policy. Finally, inquire about the relevant date range for the data involved in the dispute.

At the conclusion of the interview process, make sure each key and tangential player is aware of the need to retain documents and warn them that if they have any doubts they should ask before deleting anything.

Next, turn your attention to your storage systems. If you are well versed in the inner-workings of the system, move on to the next point. If you do not know your system inside and out, interview your IT Professionals to gain that knowledge. When it comes time to collect and preserve the data, you cannot rely upon the IT folks alone to carry out your wishes. You are responsible for understanding the system and verifying your IT Professionals are doing what you've outlined.

Finally, plan your search. In the next step you will collect the data involved in the dispute. To accomplish this, you may have to utilize searches of your system with your IT Professionals. For example, in a race discrimination case, you would clearly want to hold all emails from the offending party and those other persons involved. From there, you would still want to search the remainder of your staff members' email to attempt to locate relevant information outside the circle of key and tangential staff involved. Other racial comments, outside the scope of the individual claim, will be relevant. Appropriate search terms might include the basis of the discrimination, expletives, and other derogatory phrases.

Step 2: Collect. With your interviews complete and your search terms identified, you are ready to start collecting the data that will ultimately be culled by counsel for production in litigation. Remember, the goal at this stage is to retain *more* data than you will produce. You want to cast a *wider* net than you will need to avoid missing anything. Create repositories for your paper and electronic documents. Consider scanning paper documents so that they will be easier to access, catalog, and evaluate before production. Make sure that those collecting the data understand the importance of their work. Also arrange to obtain documents from outside sources such as auditors, accountants, payroll companies, attorneys from prior matters, and other sources that are unique to your business.

[25] Don't assume interviewees realize the importance of disclosing that there is information stored on their home computer or a flash drive.

[26] *Williams v. Sprint/United Mgmt Co.*, 230 F.R.D. (D. Kan 2005).

It is imperative that you and your IT Professionals understand one another in completing this task. One of the biggest sources of difficulty in creating an effective litigation hold is misunderstanding and miscommunication between owners and IT Professionals. When deposed by an attorney with understanding of technical aspects of computers or servers, IT Professionals have been known to identify additional sources of data that business owners did not know about, despite the owner's attempts to learn everything during the process of investigating claims – so be wary! Trudging on, we've got to revisit the difference between accessible and inaccessible data discussed above.[27] There is uncertainty about whether you have to keep "inaccessible" data as part of your litigation hold. Neither Texas state courts nor federal courts in and over Texas have addressed whether inaccessible back-up tapes must be kept as part of a litigation hold.[28] For this reason, you will have to keep in mind the data which exists on those tapes in analyzing the scope of your hold.

With the assistance of your IT Professionals, make decisions about "metadata" and how it will be protected. Metadata is data about data – as if this process were not complicated enough. To use an example, a word processing document is full of "data," but the computer program always keeps data about the document connected to it. The metadata is information about when the document was last edited, what the last red-line changes were, who worked on it, how long it was open, etc. While this information is often not important in litigation, it can prove important in certain circumstances. For example, when someone alleges they created a document at a certain time, but did not. The metadata would help provide that information and has been known to prove a case all together.

Run your searches. Work with your IT Professionals to run the searches for the terms developed as part of your investigation. Make sure that the searches and all document collection efforts are taking place at *all* locations of your company. Failing to institute the hold at a separate office can be the cause of sanctions or other penalties implemented by the court.[29]

Step 3: Follow up. This is a short, but vital, step in the process. A litigation hold requires constant attention. Not only do you have an obligation to collect data that exists at the time the hold goes into place, but also information that develops after the hold is put in place. Of course, there will not usually be a lot of new data because claims tend to involve things that happened in the past, but you have a duty to keep any new data. You must make sure the data is collected and that all staff is regularly reminded of their obligation to set aside information that is part of the hold. If you fail to meet this obligation, you can again find yourself in the cross-hairs of the court. In at least one instance, a company put an electronic warning up on all staff member's computer each time they logged in to remind them of the hold. This may be over-kill, but it illustrates the point. Keep records of your follow-up efforts and consider making the follow-up reminders to staff via email or other written form so you will be able to show a court your efforts.

---

[27] Note, some companies do not have separate disaster recovery tapes and only have "accessible" back-up tapes. If this is the case, there will not be a separate need to keep disaster recovery tapes because there are none!

[28] *Zubulake v. UBS Warburg LLC*, 220 F.R.D. 212, 218 (S.D.N.Y.2003) ("inaccessible data" not required to be kept in normal course of business); *but see Treppel v. Biovail Corp.*, 249 F.R.D. 111 (S.D.N.Y. 2008).

[29] *Zubulake v. UBS Warburg LLC*, 229 F.R.D. 422 (S.D.N.Y. 2004).

Step 4: Make a Deal.[30] It is placed here because it is most likely to happen at this juncture, but this step could happen at any time in the hold process. Opposing counsel's appearance could be the first time you reasonably anticipate litigation. Nonetheless, as soon as opposing counsel is involved, strike a deal – in writing – on the parameters of electronic discovery. The potential benefits are innumerable, but certainly include: (1) possibly allowing you to delete data outside the scope you have agreed upon; (2) enabling you to force the opposing party to become responsible for electronic documents they possess which may benefit your case; and (3) providing certainty as to your obligations, so that you are not subject to the whim and mercy of a judge to determine whether you have done what is required.

For your own protection, however, the process needs to be as detailed as your litigation hold would have been, or is. If you fail to make an agreement covering a category of information, and subsequently delete it, you will have serious problems explaining it to the court. Remember in negotiating the agreement, however, that a little finesse is required. If you have followed my program, you will know what opposing counsel *should* want. Of course, opposing counsel may not be so organized. Don't just give up the fort! Make the opposing party ask you for it. If he or she never figures it out, you may be off scot-free. Utilize the following as a guide in preparing the agreement:[31]

⇒ What will be preserved? The considerations in this area need to be as broad as your litigation hold. Go through all of the document categories identified above in both the paper and electronic categories. You need to agree whose information will be protected, including key and tangential players.

⇒ How will the data be preserved? This is your opportunity to learn the opposing party's computer system. Ask how data is stored, where it is stored, who is responsible for it, and how long it is kept. This information will be useful in determining what information *you* want to ask for and how you want it produced. It also serves the purpose of allowing you to determine whether data will be produced on paper, saved as PDF files, or in a format that would allow someone to open it in the original program. Remember to consider whether the opposing party's information may include valuable metadata which could be used to prove an aspect of your case. If it might, specify that the information be produced with metadata in its original or "native" format.

⇒ What will be the date range preserved? How far back does the dispute go back? How far do the documents from which the dispute arises go back? Could it be that you need different date ranges for different types of data? Perhaps you need word processing documents back to the time of the transaction and emails within the last 2 years? Don't ever agree to have an end to the date range. If, for example, the opposing party's staff members want to write emails about the claim while litigation is going on, you don't want to give up the opportunity to get the data.

[30] For the business owners reading this guide, do not attempt this on your own. Have your counsel handle the negotiations, but make them aware of your desire to consider these points.
[31] For additional guidance, review Fed. R. Civ. P. 26(f), and, more importantly, its commentary (even in state court cases this will be helpful).

⇒ What will the search terms be? You don't want to agree to produce every single email for a person because it will have two consequences: (1) your attorney will have to review it and charge you to do so (discussed below); (2) it will cost more money to produce because there are more pages. Agree to search phrases regarding emails that result in the discovery of all relevant emails. Remember though, not to allow the opposing party to delete anything outside the search parameters because the documents they produce may lead you to new search terms. If you allow them to delete this data there will be nothing left once you realize its importance.

Step 5: Utilize and Produce Data. You might think this would be the simplest step. Package up what you've pulled together and send it on. Regrettably, that is not the case. Producing the data may be the most costly and time consuming part of the process. Once the data is collected, it should be reviewed by counsel for attorney-client, work-product, and other privileges, in addition to other objections, before being produced to the opposing party.

Some commentators believe changes in rules and statutes over the last few years eliminate some, or the entire burden, of reviewing documents. I disagree. The law provides a safe harbor for pulling back information only under certain circumstances; but it should not be utilized as a crutch to avoid document review. Under these "claw-back" or "snap-back" provisions, you can retrieve privileged information that has been inadvertently produced.

The applicable federal rule for this is Federal R. Ev. 502(b) which governs inadvertent disclosure and provides that there is no waiver of privilege if: (1) the disclosure is inadvertent; (2) the holder of the privilege or protection took reasonable steps to prevent disclosure; and (3) the holder promptly took reasonable steps to rectify the error, including (if applicable) following Federal Rule of Civil Procedure 26(b)(5)(B).[32] The applicable Texas rule is Tex. R. Civ. P. 193.3(d) which provides that privileges are not waived by production if: within ten days or a shorter time ordered by the court, after the producing party actually discovers that such production was made – the producing party amends the response identifying material or information produced and stating a privilege is asserted.[33],[34],[35],[36]

---

[32] Fed. R. Ev. 502(b) became effective in September 2008. Understandably there are no cases in Texas federal district courts or the 5th Circuit interpreting it.

[33]TRCP 193.3(d) Privilege Not Waived by Production. A party who produces material or information without intending to waive a claim of privilege does not waive that claim under these rules or the Rules of Evidence if--within ten days or a shorter time ordered by the court, after the producing party actually discovers that such production was made--the producing party amends the response, identifying the material or information produced and stating the privilege asserted. If the producing party thus amends the response to assert a privilege, the requesting party must promptly return the specified material or information and any copies pending any ruling by the court denying the privilege.

Tex. R. Civ. P. 193, Comment 4 (1999): Rule 193.3(d) is a new provision that allows a party to assert a claim of privilege to material or information produced inadvertently without intending to waive the privilege…. The focus is on the intent to waive the privilege, not the intent to produce the material or information. A party who fails to diligently screen documents before producing them does not waive a claim of privilege. This rule is thus broader than Tex. R. Evid. 511 and overturns *Granada Corp. v. First Court of Appeals*, 844 S.W.2d 223 (Tex. 1992), to the extent the two conflict. The ten-day period (which may be shortened by the court) allowed for an amended response does not run from the production of the material or information but from the party's first awareness of the mistake. To avoid complications at trial, a party may identify prior to trial the documents intended to be offered, thereby triggering the obligation to assert any overlooked privilege under this rule.

[34] TRCP 193.3(d) has been held not to apply to third-party discovery responses. *In re Ortuno*, 2008 WL 2339800 (Tex. App.—Houston [14th Dist.] 2008).

Do not to rely solely upon these rules, because each is subject to the discretion of a judge. You cannot rest decisions about whether you can "unproduce" privileged information upon a judge that might not feel it is appropriate to do so – especially if you decided not to review documents at all before producing them. What is more, opposing counsel will certainly look at the documents and then try to come up with a way to get the information legitimately. Finally, most attorneys don't consider that the right to claw-back in Texas could be ineffective as to litigation in other states. In the other state, a judge might find that the documents produced do not retain their privilege and, once produced, are available for use in different litigation in that state. You're better off knowing the claw-back rule is there for the worst case scenario, than relying on it to reduce document review costs.

In addition to review for privilege, you must take care to redact the confidential and private information of others, whose information you may produce.[37] For example, in the employment discrimination context, you might be producing staff HR files of individuals involved in the case. You must remember to redact their confidential information, such as social security numbers. In a different circumstance, you may be producing patient records from your medical files. In this instance you must make sure to comply with HIPAA. Other sensitive information to look for includes trade secrets for your business, or others, and drivers licenses.

The costs associated with document review can comprise many attorney hours depending on the number of documents. In this circumstance, you should consider contacting a firm specializing in e-discovery assistance to determine whether their document review processes (some have lawyers in India to do document review for less money) and pricing make it worthwhile not to utilize your attorneys for that purpose. There are pluses and minuses to this approach which your attorney can help you understand. If nothing else, these firms may be able to help you de-duplicate the data, which is to eliminate duplicate emails and documents to reduce the total number of documents your attorney will review.

With document review complete, you can wipe the sweat from your brow, produce the information, and move on, right? Wrong, again. One of the most valuable things that will arise from your collection of all of this data is the opportunity to utilize it to prepare witnesses for depositions. It is imperative that witnesses review relevant documents *before* their depositions so that they do not testify based on memory alone. The witness could end on the receiving end of a right-hook from the opposing attorney when he pulls out a contradictory email that the witness did not get to review before the deposition. Make certain to use your hard work to your benefit. If you don't institute the litigation hold process early, you may not have the documents collected before depositions begin.

---

[35] TRCP 193.3(d) has been held to include work-product privileged material. *In re O'Quinn*, 2008 WL 173256 (Tex.App.—San Antonio 2008).

[36] TRCP 193.3(d) has been held to apply to documents inadvertently provided to a party's expert witness so long as that expert witness does not testify at trial. *In re Christus Spohn Hosp. Kleberg*, 222 S.W.3d 434 (Tex. 2007).

[37] Disclosure of confidential third-party information has been discussed by the Texas Supreme Court, but not decided. *In re CI Host*, 92 S.W.3d 514, 517 (Tex. 2002).

ABOUT THE AUTHORS

Michael Kelsheimer

Michael Kelsheimer's practice focuses on commercial and employment litigation. His experience as a former briefing attorney for the United States District Court coupled with his extensive experience in commercial and employment disputes has enabled Michael to successfully secure favorable verdicts and judgments in a wide variety of commercial cases for businesses and professionals engaged in multiple industries as well as the defense of all types of lawsuits. Michael's efforts have included cases involving race and sex discrimination, collections, deceptive trade, employment discrimination, fraud, fraudulent transfer, negligence, real estate titles, and enforcement of contracts in state and federal courts as well as through binding arbitration.

Contact Information: mkelsheimer@lrmlaw.com or call 214.237.6346

Jason Rodriguez

Jason serves as an IT Manager and has overseen complex technical migrations and implementations as the firm has grown over the last several years. Presently he is overseeing the implementation of a document management system for the firm. Jason has a degree in management information systems, holds MCSA and ICSE certifications and several others. Additionally, he is presently taking courses to achieve an additional Associate's Degree in paralegal studies.

Contact Information: jrodriguez@lrmlaw.com or call 214.237.6314

FEDERAL REGULATIONS

Age Discrimination in Employment Act (ADEA)
Americans with Disabilities Act (ADA)
Civil Rights Act of 1964, Title VII
Consolidated Omnibus Budget Reconciliation Act (COBRA)
Davis-Bacon Act
Employee Polygraph Protection Act
Employee Retirement Income Security Act (ERISA)
Equal Pay Act
Equal Pay Act and the Fair Labor Standards Act
Executive Order 11246
Fair and Accurate Credit Transactions Act (FACTA)
Fair Labor Standards Act (FLSA)
Family & Medical Leave Act (FMLA)
Federal Income Tax Withholding
Federal Insurance Contribution Act (FICA)
Federal Unemployment Tax (FUTA)
Immigration Reform & Control Act (IRCA)
Occupational Safety & Health Act (OSHA)
OSHA No. 200-S) [Editor Note: After 1/1/2002, OSHA No. 300 A
Rehabilitation Act of 1973
Service Contract Act
The Employee Polygraph Protection Act
The Uniform Guidelines on Employee Selection Procedures (UGESP) provide guidance for employers subject to Title VII or Executive Order 11246
Vietnam Era Veterans' Readjustment Assistance Act.
Walsh-Healy Public Contracts Act
Bankruptcy Laws
Sarbanes-Oxley
Securities Exchange Act