



**TO SHRED OR NOT TO SHRED:
Document Retention Policies and Spoliation
Issues in a Digital Age**

by
Andrew Pearce, Attorney at Law
Sara Richey, Attorney at Law

To Shred or not to Shred: Document Retention Policies and Spoliation Issues in a Digital Age

Today, more than ever, documents and information are created and stored electronically. With many companies going “paperless,” the issue of how to handle all of this electronically stored data is increasingly becoming a dilemma. Should we just keep everything forever because it isn’t taking up space in hundreds of boxes or files around the office? The clear answer is no. Just as with traditional hard copy documents, companies need to implement electronic document retention policies to save money on storage and to prevent discovery sanctions in future litigation. It is no longer just a progressive idea to have a retention policy for electronic documents, it is a business necessity.

Increasing amount of electronic data

The amount of electronic data created and stored is increasing not only in sheer volume but also in the type. Discoverable electronic information not only includes word documents and emails, but also other data such as powerpoint presentations, photos, Facebook postings, videos, and blogs. Companies need to be aware of the electronic footprint their employees are creating when drafting a retention policy.

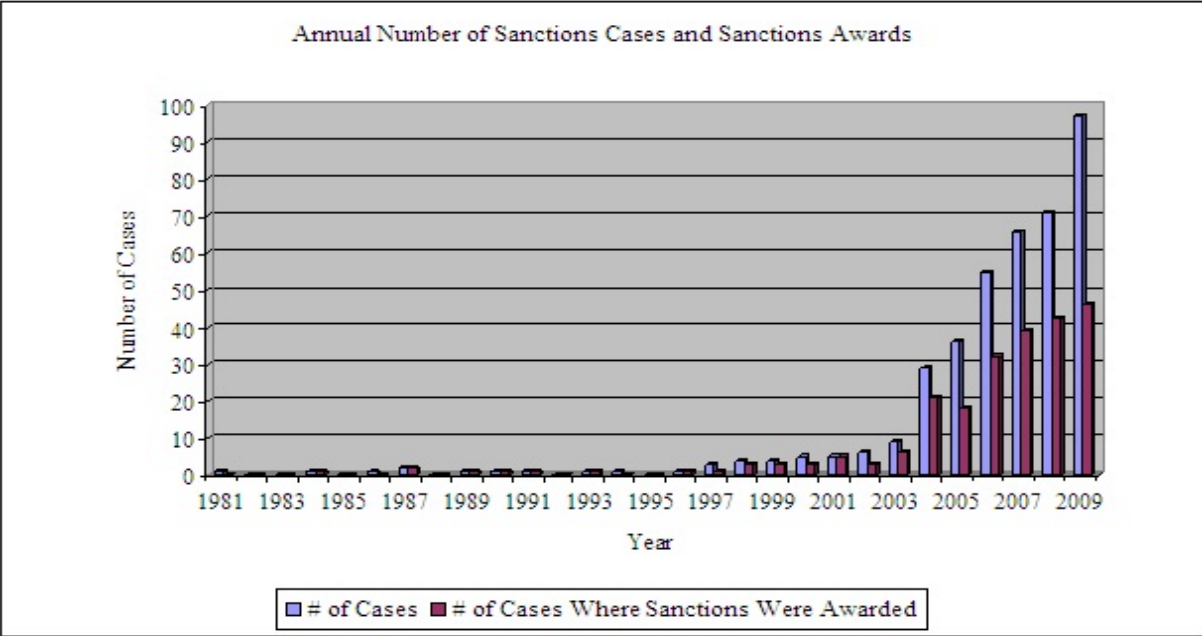
	<u>2009¹</u>	<u>2010²</u>
Emails		
• The number of emails sent annually:	90 trillion	107 trillion
• Average number of email messages per day:	247 billion	294 billion
• The number of email users worldwide:	1.4 billion	1.88 billion
Social media		
• The number of blogs on the Internet:	126 million	152 million
• People on Facebook:	350 million	600 million
Images		
• Photos hosted by Flickr:	4 billion	5 billion
• Photos uploaded each month to Facebook:	2.5 billion	3+ billion

Likewise, the punishment for a company’s failure to properly retain documents is becoming increasingly more severe.³

¹ <http://royal.pingdom.com/2010/01/22/internet-2009-in-numbers/>.

² <http://royal.pingdom.com/2011/01/12/internet-2010-in-numbers/>.

³ Dan H. Willoughby & Rose Hunter Jones & Gregory R. Antine, *Sanctions For E-Discovery Violations: By The Numbers*, 60 Duke L.J., 790, 795 (2010).



Sanctions against parties for spoliation of evidence can include dismissals, adverse jury instructions, and significant monetary awards. Even so, the meteoric increase of electronically stored information (ESI) in all of its formats — laptops, desktops, instant messaging, smart phones, etc. — has made efforts by companies to develop and maintain sufficient document retention policies increasingly difficult. Further complicating the matter is the potential cost involved in developing and implementing a policy, as well as the lack of a uniform set of regulations or laws covering document retention.

It is also important to remember that electronic data and documents are often stored in multiple places. A simple example of this is email. Both the sender and every recipient have copies of the message stored on their computer or server. Even if the sender’s company routinely destroys emails according to a retention policy, the email message may be discoverable because a redundant copy exists with the recipients. The lesson here is that just because you destroy your copy of an electronic document does not mean it is really gone forever. It is virtually impossible to destroy every copy of an electronic document that has been sent or posted via the internet. That can be an important issue to consider when going through the discovery process.

Despite the inherent difficulty, in today’s world of social media, every company with more than two employees should develop a social media policy. Likewise, a document retention policy is both necessary and beneficial for a number of reasons, including a company’s ability to maintain and preserve important records needed for ongoing business, as well as the ability to anticipate, budget and control costs associated with document retention and storage. Further, in the context of litigation, an ESI document retention policy will protect a company from potential spoliation sanctions, while also enabling the company to readily access data that might be exculpatory, or at least, supportive of the company in defense of a claim.

The Need for a Social Media Policy

A social media policy serves several purposes, including, but not limited to: (1) educating your workforce on the various types of social media outlets; (2) determining how social media can be used to further your company's business interests; and (3) establishing guidelines for using social media consistent with your company's core values and/or code of conduct.

With this in mind, the best way to start is by not trying to recreate the wheel — several large institutions have social media policies in place that provide a good template for any company to draw from. You can find a number of these policies at:

www.socialmediagovernance.com/policies.php

Armed with this information, you should form a small committee from different constituent groups within your company to evaluate the various policies. Establish a system to determine what portions of each policy will work for your company given the industry you serve as well as how your company operates. Part of the process should include interviewing your employees to determine which social media outlets they regularly use and how they think using social media can help or hurt the company's ability to accomplish its goals.

Obviously, before any policy is finalized you should make sure that the legal implications are addressed. For example, you want to make sure your employees avoid violating any advertising laws your company may be bound by, guard against employees making defamatory statements or infringing upon intellectual property rights of others, and address privacy concerns. The one legal issue all policies should cover is consequences for violating the policy. This will become an issue if an employee should be terminated because of their conduct on a social media outlet.

The Need for a Document Retention Policy

Like social media policies, there is both a need to establish a method for the efficient, consistent and effective management of ESI, as well as a multitude of ways that companies can create such a document retention policy regarding ESI. The need can be seen in the Federal Rules of Civil Procedure, which now expressly recognize ESI as a form of discoverable information in litigation and require litigants to discuss the preservation and production of ESI at the outset of each case. To effectively meet these requirements, litigants must have full command of the content, location and format of their ESI, as well as the ability to quickly assess whether any ESI is confidential or privileged.

In the event of litigation, under FRCP Rule 34(b), a requesting party is allowed to specify a form or forms of production – i.e. paper, TIFF, native, etc. The producing party must then produce in the format requested, or object to requested form or forms. If a party objects, then the objecting party must state the form or forms it intends to use in production. If the requesting party does not specify a form or forms of production, the producing party must produce ESI in one of the following forms: (1) in the way it is ordinarily maintained in the usual course of business, or (2) in a reasonably usable form or forms, i.e. searchable format.

It is also worth noting that a producing party cannot convert ESI from a form in which it is ordinarily maintained to a form that makes it difficult or more burdensome for the

requesting party to use the information. Additionally, if the ESI is normally maintained in a searchable way, the producing party cannot remove or degrade searchable features. However, under Rule

Rule 26(b)(2)(B), a party need not provide discovery of electronically stored information from sources that the party identifies as not reasonably accessible because of undue burden. Examples of data not reasonably accessible include: backup tapes intended for disaster recovery purposes, legacy data that remains from obsolete systems and is unintelligible on successor systems, data that was deleted but remains in fragmented form, and databases designed to create particular information in certain ways and that cannot readily create other types or forms of information.

In Texas, under Texas Rule of Civil Procedure 196.4, a requesting party must specifically identify the requested information and also specify the form in which that data should be produced. Unless otherwise ordered, the responding party need only produce data that is reasonably available in the ordinary course of business in reasonably usable form. For any electronic data requiring extraordinary steps for retrieval or production, the court should enter a cost-shifting order directing the requesting party to pay the reasonable expenses.

Considerations when Drafting an ESI Policy

Data retention requirements depend on the type of data and the purposes for which it is used, as well as the parties involved in the transactions for which the documents and data were generated. Therefore, a company looking to implement data retention and archival policies needs to analyze state, federal, and international rules, laws, and regulations, as well as the contracts to which it is a party and self-regulatory organizations to which the company belongs to determine the length of time the company is required to retain data and documents. A company should also look at its internal business needs when making such a decision.

A. Legal Concerns

In addition to the litigation aspects of ESI, additional minimum records retention requirements vary by state and by data type, but typically range from three years to permanent retention. Some of the main sources of rules, laws, and regulations for data retention and archival are audit and tax, securities, employment, and health and privacy related laws. For example, Sarbanes Oxley contains numerous document retention requirements for publicly traded companies, and the Health Information Privacy Act and Health Insurance Portability and Accountability Act contain numerous requirements related to healthcare and insurance related documents. Special requirements also apply when you contract with government agencies. These requirements must be strictly followed, may be more strenuous than required by states and other agencies, and often times depend on the agency involved (i.e. the Department of Defense has additional rules that don't apply to all government agencies).

Depending on the nature of your business, there may be other agencies that have their own special requirements. For instance, OSHA requires that certain industrial hygiene records and medical records be retained for 30 years. As an additional example, in the

state of Texas, disability and sick benefit records must be retained for 6 years and claims of employee inventions must be retained for 25 years.

There are likely hundreds of other laws, rules, and regulations that could apply to document and data retention and archival. As such, it is important for a company to know the industries in which it is involved, the organizations it belongs to, and the clients and customers whom the company works with in order to be able to determine what rules, regulations, and laws are applicable.

The most prominent current concern for companies in the United States is compliance with new Federal Rules of Civil Procedure relating to document retention that apply in every lawsuit filed in United States federal courts. Many states have also adopted provisions similar to those found in the Federal Rules of Civil Procedure. Under these new rules, a company must be vigilant about preserving any data or documents in its possession, custody, or control that might be relevant to the litigation.

In developing procedures for compliance with the Federal Rules of Civil Procedure, it is important to remember that all information pertinent to a lawsuit may have to be retrieved and turned over to the opposing party (or even possibly government officials) during litigation cases regardless of the medium such as paper, hard disk or tape.

B. Business Concerns

In addition to legal requirements, businesses may have their own data retention requirements that can range from contractual obligations with customers or suppliers to administrative or operational information such as policies and procedures that define daily functions. Each business must set their own data retention requirements to sufficiently maintain their business operations. Day to day business activities often dictate the length of time information needs to remain accessible.

The goal is to keep the information that is necessary to run the business and delete the “unnecessary” information. That said, under no circumstances should information be deleted just because you think it might hurt the company if discovered at a later date. If the company has a data retention policy (which is discussed in Section C below), stick to the policy. A balance must be struck between reasonable expectations, business needs, and the need to protect companies and individuals from unlawful acts such as fraud and threats to their corporate and personal well being.

C. Data Retention Policies

Data retention policies are useful documents that deal with the complex issues of maintaining corporate information for a pre-determined length of time. In general, a document retention policy should:

- State the purpose of the policy;
- Define who is effected by the policy;
- Identify what type of data and electronic systems are covered by the policy;
- Define key terms (especially legal and technical terminology);
- Describe the requirements in detail from the legal, business and personal perspectives;
- Outline the procedures for ensuring data is properly retained;
- Outline the procedures for ensuring data is properly destroyed;

- Clearly document the litigation exception process and how to respond to discovery requests;
 - List the responsibilities of those involved in data retention activities;
 - Build a table showing the information type and its corresponding retention period;
 - Document the specific duties of a central/corporate data retention team if one exists; and
- Include an appendix for additional reference information, as needed.

The considerations involved in drafting a policy include:

1) *What types of data and records should be covered?*

- Electronically stored information includes emails, text messages, and other business related information generated, stored, or transmitted via a personal computer, laptop, PDA, cellular phone, or other electronic voice and data communications devices.
- Electronically stored information also includes “embedded data” or “embedded edits” and “meta-data.”

2) *What do companies need to know about their electronic information systems?*

- The type of information that is created by their computer systems;
- How that information is stored;
- Where the information is stored;
- How long the information is stored;
- How the information is accessed; and
- How the information is overwritten, deleted, and destroyed during the normal operation of the system.

3) *What measures should companies take when drafting an ESI policy?*

- Inventory all electronic storage systems and gain an understanding of where information is located and how it is stored and generated on the various systems.
- Implement retention and destruction policies for electronic records.
- Implement procedures for placing a “litigation hold” on any electronic records that may be relevant to litigation and discoverable in litigation including notification procedures to ensure that ESI is not overwritten or deleted (commonly called “Preservation Notices”). A Preservation Notice must be sent out to all employees who may have or have access to relevant information. Once a Preservation Notice is issued, document destruction must cease for all classes of documents that may contain relevant information. A sample Preservation Notice is attached.
- Educate and train employees on policies relating to electronic records and compliance with Preservation Notices.
- Involve IT personnel in designing policies and training employees to ensure that IT personnel understand the objectives and consequences.

Different types of data require different lengths of retention. Organizations should therefore develop a retention schedule that defines record types and sets minimum

retention periods for records series of each type (and where appropriate, these schedules should also set maximum time periods for retention). In addition to describing how long various types of information must be maintained in your possession, retention policies usually describe the procedures for archiving the information, guidelines for destroying the information when the time limit has been exceeded, and special mechanisms for handling the information when involved in litigation.

Also, a company must also consider the costs — in terms of both money and time — involved in implementing and maintaining the policy. Some employees are diligent in keeping every document that comes across his or desk, including every email sent or received, while others delete or otherwise destroy all business documents and communications. From the outset, it is critically important that a company's management embraces both the implementation of the policy, as well as the policy's consistent enforcement. Likewise, a company cannot maintain an effective ESI policy without understanding the types of data created by its employees, where such data is stored, and what the retention policy is for such data.

Consistent implementation of the policy is also critically important because such consistency shows a good faith legal compliance. Conversely, the sporadic or random enforcement of a retention policy could be used as evidence of intentional destruction in the event of litigation or investigation. A suggested element of the retention policy is to require approval prior to destruction to ensure that the records are not subject to a legal.

Spoliation

Spoliation is defined as “the improper destruction of evidence relevant to a case.”⁴ “Intentional spoliation of evidence relevant to a case raises a presumption that the evidence would have been unfavorable to the cause of the spoliator.”⁵ However, the presumption may be rebutted if the alleged spoliator shows that the “evidence in question was not destroyed with fraudulent intent or purpose.”⁶

The purpose of the spoliation rule is to prevent a party from subverting the “discovery process and the fair administration of justice simply by destroying evidence of an adverse claim.”⁷ Thus, once a party is aware of a potential claim, that party incurs a “duty to exercise reasonable care to preserve information relevant to that claim.”⁸ If a party breaches that duty by intentionally or negligently failing to preserve relevant evidence, that party may be held accountable for its loss.⁹ Such accountability may be achieved through sanctions or a spoliation instruction.¹⁰

Procedurally, the trial court evaluates a spoliation motion by first considering: (1) whether a duty existed to preserve the evidence; (2) whether the evidence was

⁴ *Cardoza v. Reliant Energy HL&P*, No. 01-03-01126-CV, 2005 WL 1189649, at *2 (Tex. App.—Houston [1st Dist.] May 20, 2005, no pet.).

⁵ *Ordonez v. M.W. McCurdy & Co., Inc.*, 984 S.W.2d 264, 273 (Tex. App.—Houston [1st Dist.] 1998, no pet.).

⁶ *Id.*

⁷ *Offshore Pipelines, Inc. v. Schooley*, 984 S.W.2d 654, 666 (Tex. App.—Houston [1st Dist.] 1998, no pet.).

⁸ *Id.*

⁹ *Id.*

¹⁰ *Id.*

negligently or intentionally spoliated; and (3) whether the spoliation prejudiced the other party's case.¹¹

Whether a Duty Existed

A duty to preserve evidence exists when “a party knows or reasonably should know that there is a substantial chance that a claim will be filed and that evidence in its possession will be material and relevant to that claim.”¹² An objective test for anticipation of litigation is whether a reasonable person would conclude from the circumstances that there was a substantial chance for litigation.¹³ The Texas Supreme Court has made clear that *actual notice* of the potential for litigation is not required; instead, “*common sense* dictates that a party may reasonably anticipate suit being filed....before the plaintiff manifests an intent to sue.”¹⁴ Thus, “a party should be found to be on notice of potential litigation when, after viewing the totality of the circumstances, the party either actually anticipated litigation *or* a reasonable person in the party's position would have anticipated litigation.”¹⁵

Whether the Evidence was Negligently or Intentionally Spoliated

An alleged spoliator can explain the reason for the evidence's destruction; for example, a party could argue the “the destruction of the evidence was beyond the spoliator's control or done in the ordinary course of business.”¹⁶ However, although a spoliator can defend against an allegation of negligent or intentional destruction of evidence by providing other explanations for the destruction (such as the destruction was beyond the spoliator's control or done in the ordinary course of business), if the duty to preserve evidence arises before the destruction, such defenses will not excuse the spoliation.¹⁷

Whether the Spoliation Prejudiced the Other Party's Case

Under the prejudice prong, Texas courts analyze a variety of issues, “including the relevancy of the missing evidence, the harmful effect of the evidence, and the availability of other evidence to take the place of the missing information.”¹⁸ The most important factor for a court to consider is “the destroyed evidence's relevancy,” but a court should also consider “whether the destroyed evidence was cumulative of other competent evidence that a party can use in place of the destroyed evidence, and whether the destroyed evidence supports key issues in the case.”¹⁹ The mere fact that evidence was destroyed is some evidence of its relevance, and when dealing with *intentional* destruction of evidence, a court should find the destructed evidence was relevant and harmful to the spoliator's case absent evidence to the contrary.²⁰ If the trial court finds the existence of a duty, a breach and a prejudice to the other party, it must then “consider what remedy is warranted by the circumstances of the case” and, in

¹¹ *Id.*

¹² Cardoza, 2005 WL 1189649, at *2 (internal quotations omitted).

¹³ *Dillard*, 171 S.W.3d at 209 (holding a spoliation instruction was proper when the party seeking it established that a letter had been set to the opposing party notifying it of the accident and injuries arising from it).

¹⁴ *Trevino*, 969 S.W.2d at 956 (Baker, J., concurring) (emphasis in original) (quoting *National Tank Co. v. Brotherton*, 851 S.W.2d 193, 204 (Tex. 1993)).

¹⁵ *Trevino*, 969 S.W.2d at 956 (Baker, J., concurring) (emphasis in original).

¹⁶ *Id.*

¹⁷ *Trevino*, 969 S.W.2d at 957 (Baker, J., concurring).

¹⁸ *Offshore Pipelines, Inc. v. Schooley*, 984 S.W.2d at 666.

¹⁹ *Trevino*, 969 S.W.2d at 958 (Baker, J., concurring).

²⁰ *Id.*

doing so, is “accorded broad discretion.”²¹ In sum, a party is entitled to a remedy when the spoliation hinders its ability to present its case or defense.

What a Requesting Party Must Show

The party requesting the instruction must show that the spoliation prejudiced its ability to present its case.²²

To prove prejudice the party must show:

1. it requested the missing evidence and pursued a court order to compel its production,
2. the missing evidence is relevant,
3. there is no other evidence available to replace the missing evidence, and
4. the missing evidence supports key issues in the case.²³

What is the Appropriate Sanction for Spoliation?

Once the three-part inquiry has been satisfied, the court has broad discretion in determining the appropriate sanction or in issuing a spoliation presumption instruction.²⁴ The most severe sanction—dismissing the action or rendering a default judgment against the spoliator—is warranted when the spoliator’s conduct was egregious, the prejudice to the non-spoliator was great, and imposing a lesser sanction would be ineffective to cure the prejudice.²⁵ With respect to the spoliation presumption, it has been a part of Texas jurisprudence for over a century and finds its roots in the Latin maxim *omnia presumuntur contra spoliatorem*, meaning “all things presumed against a despoiler or wrongdoer.”²⁶ Such an instruction can be given in one of two forms, depending on the severity of prejudice resulting from the destruction: (1) a rebuttable presumption that the spoliator has either negligently or intentionally destroyed evidence and, therefore, the jury should presume the destroyed evidence was unfavorable to the spoliator; or (2) an adverse presumption that the evidence would have been unfavorable to the spoliator.²⁷

Spoliation of Evidence did Occur — *Offshore Pipelines, Inc. v. Schooley*

In *Offshore Pipelines, Inc.*, Edward Lamar Schooley (“Schooley”) sued Offshore Pipelines, Inc. and OPI International, Inc. (collectively, “Offshore”) for personal injuries allegedly sustained while employed as an electrician onboard an Offshore vessel.²⁸ Specifically, Schooley alleged that he developed an intestinal tumor due to the vessel’s contaminated drinking water.²⁹

Schooley sought Offshore’s medical logs for the time period in issue.³⁰ In response, Offshore’s corporate officer testified that although he had not instructed anyone to

²¹ *Offshore Pipelines, Inc. v. Schooley*, 984 S.W.2d at 666.

²² *Offshore Pipelines, Inc. v. Schooley*, 984 S.W.2d at 666 (citing *Trevino* 968 S.W.2d at 957 (Baker, J., concurring))

²³ *Id.*

²⁴ *Trevino*, 969 S.W.2d at 953.

²⁵ *Trevino*, 969 S.W.2d at 959 (Baker, J., concurring).

²⁶ *Wal-Mart*, 106 S.W.3d at 721.

²⁷ *Trevino*, 969 S.W.2d at 960 (Baker, J., concurring).

²⁸ *Id.* at 657.

²⁹ *Id.* at 660.

³⁰ *Id.* at 666.

destroy the logs, he had been unable to locate them and that “many records” had been removed from the vessel during a subsequent trip.³¹ Further, the corporate officer testified that he did not think it “curious or unusual” that Offshore had retained all of the vessel’s logs except the medical log covering the period of time in question.³² As a result, the trial court included the following spoliation instruction: “If a party fails to produce evidence which is under its control and reasonably available to it and not reasonably available to the adverse party, then you may infer that the evidence is unfavorable to the party who could have produced it and did not.”³³

Offshore appealed, arguing that that the trial court “abused its discretion in giving the spoliation instruction because ‘the spoliation rule applies only when evidence has been *intentionally* destroyed, not merely lost.’”³⁴ The First Court of Appeals noted, however, that following a trial court’s preliminary hearing to determine the parties’ “reasons for the unavailability of the evidence, the importance of the missing evidence, and the availability of other cumulative proof,” the trial court was within its broad discretion to determine a party breached its duty to preserve evidence, either negligently or intentionally, and that the loss of the evidence prejudiced the other party.³⁵ As a result, the court was within its discretion to decide a spoliation instruction was proper.³⁶

Spoliation of Evidence did not Occur — *Ordonez v. M.W. McCurdy & Co., Inc.*

In *Ordonez*, a van driven by Robert Ordonez (“Ordonez”) was struck by a truck driven by Arthur Johnson (“Johnson”), an employee of M.W. McCurdy & Company (“McCurdy”).³⁷ As a result, Ordonez filed suit, alleging that Johnson was negligent and negligent per se and that McCurdy was vicariously liable for Johnson’s conduct.³⁸

The issue of spoliation was raised when Ordonez claimed that McCurdy intentionally destroyed logbooks documenting hours driven and off-duty time, as required by federal regulations.³⁹ A McCurdy representative testified that logbooks only were only retained for six months according to standard company procedures.⁴⁰ The representative further testified that the relevant logbooks were destroyed pursuant to this procedure, but Ordonez elicited testimony that the relevant logbooks were destroyed even though McCurdy had *possibly* received notice of Ordonez’s intent to file a claim related to the wreck.⁴¹

Ordonez argued this testimony was “unequivocal evidence” that McCurdy intentionally destroyed the logbooks.⁴² The First Court of Appeals disagreed, noting that the representative “merely testified the log book was ‘thrown away’ and that it was ‘possible’

³¹ *Id.*

³² *Id.*

³³ *Id.*

³⁴ *Id.* at 667.

³⁵ *Id.* at 667-68.

³⁶ *Id.* at 668.

³⁷ *Ordonez*, 984 S.W.2d at 273.

³⁸ *Id.*

³⁹ *Id.*

⁴⁰ *Id.*

⁴¹ *Id.*

⁴² *Id.* at 273.

that McCurdy received a notice letter from Ordonez soon after the accident.”⁴³ This testimony, coupled with the earlier testimony that all logbooks are routinely disposed of after six months, showed “only that the logbooks were thrown away pursuant to McCurdy's normal business practice of keeping such logs for only six months.”⁴⁴ As a result, the First Court of Appeals affirmed the trial court’s finding that Ordonez was not entitled to a spoliation instruction because nothing indicated the evidence was destroyed “for the purpose of concealing.”⁴⁵

Conclusion

While the task of drafting a retention policy is daunting, it can save businesses immeasurable time and money down the road. Every company should know what information it has, where it is stored and how long to keep it. Society’s transition into the digital age is showing no signs of slowing down. Every year there will be more electronic data created and stored in new and unimaginable ways. The only sound and forward thinking business decision is to spend the resources now to develop a policy and to stay ahead of the curve.

⁴³ *Id.*

⁴⁴ *Id.* at 274.

⁴⁵ *Id.*