

ASSEMBLING THE ELECTRONIC EVIDENCE TRIAGE TEAM:

**WHEN, WHAT, AND HOW TO
PRESERVE ELECTRONIC EVIDENCE**

(and what could happen if you get it wrong)

JEFFREY J. JOYCE

Jones Day*
2727 North Harwood Street
Dallas, Texas 75201
(214) 220-3939
jjjoyce@jonesday.com

*The views expressed in this paper are solely those of the author and are not intended to reflect the views or position of Jones Day, any of its other partners or attorneys, or any of its clients.

TABLE OF CONTENTS

	Page
I. INTRODUCTION	1
II. WHEN AND HOW IS THE DUTY TO PRESERVE ELECTRONIC EVIDENCE TRIGGERED?.....	2
A. Litigation, Investigations, and Other Disputes.....	2
1. Actual or Anticipated Litigation	2
2. Preservation Letters and Preservation Orders	4
3. Documents in Your Client’s “Possession, Custody, or Control”	4
B. Statutory and Regulatory Obligations.....	5
C. Business Needs	6
III. WHAT ELECTRONIC EVIDENCE MUST BE PRESERVED?	6
A. Key Differences Between Paper Documents and Electronic Evidence	6
B. All Relevant, Non-Duplicative Electronic Evidence Should Be Preserved.....	7
C. Electronic Evidence That May Not Have To Be Preserved.....	7
1. Back-Up Tapes.....	8
2. “Deleted” Electronic Evidence	8
3. Duplicative Paper and Electronic Evidence.....	9
IV. WHAT STEPS SHOULD BE TAKEN TO COMPLY WITH THE DUTY TO PRESERVE ELECTRONIC EVIDENCE?	9
A. Assemble The Electronic Evidence Triage Team.....	10
B. Take Prompt Action.....	10
C. Identify Relevant Electronic Evidence.....	10
1. Learn Your Case	10
2. Learn Your Client, Its Business, And The Key Personnel.....	11
3. Learn Your Client’s Computer Systems And IT Personnel.....	11
4. Learn Your Client’s Litigation History.....	12
D. Communicate Early and Often With Opposing Counsel and Court	12
E. Suspend Relevant Electronic Evidence Destruction Activities.....	12
F. Issue Preservation Directive Governing Electronic Evidence And Related Paper Documentation.....	13
G. Document Your Actions	14
H. Consider Counter-Attack	14
I. Audit Compliance With The Preservation Plan.....	14
J. Continually Evaluate The Preservation Plan.....	15
V. WHAT COULD HAPPEN TO PARTIES WHO FAIL TO PRESERVE	15
A. Adverse Interference Jury Instruction.....	15

TABLE OF CONTENTS

(continued)

	Page
B. Civil Sanctions	15
1. Federal Sanctions Rules	15
2. Texas Sanctions Rules	16
VI. CONCLUSION	17
APPENDIX A - SAMPLE PRESERVATION DIRECTIVE	A-1
APPENDIX B - QUESTIONS FOR CLIENT REGARDING ELECTRONIC EVIDENCE.....	B-1

ASSEMBLING THE ELECTRONIC EVIDENCE TRIAGE TEAM

ABSTRACT: A party has a duty to preserve electronic evidence that is relevant to actual or anticipated litigation, a requirement that is frequently difficult to implement because electronic evidence is often subject to automatic overwriting or purging processes. To avoid sanctions, parties must respond quickly when the duty to preserve electronic evidence arises.

Your client gets sued, and the case will almost certainly involve not only e-mails and user-created electronic evidence like Word, Excel, and PowerPoint files, but also the company's transactional or operational data, such as temperature or speed measurements for a key manufacturing process, shipping data collected by high-speed bar code readers, customer complaints regarding a product, punches employees made in a time clock, pesticide application records, or internal audit files. This data is stored for different time periods in various types of databases and flat files, some active and others archived. Your client also has voice mail archives, telephone and access card data, internet usage histories, and dozens of other collections of electronic data that may relate to some aspect of the case. Your client may have offices scattered throughout the United States and other parts of the world. There are hundreds of personal desktop computers, laptops, PDAs, home computers, diskettes, DVDs, Zip disks, and other media that could contain relevant data. The company also has banks of servers in different locations and hundreds or thousands of back-up tapes and hard drives. Due to corporate mergers and divestitures, the enterprise's different computer systems may have no ability to communicate with each other. Some of the data may be stored in obsolete systems or on tapes that cannot be read with the client's existing hardware.

If relevant to actual or anticipated litigation, this electronic evidence must be preserved just as paper evidence must. The difficulty from the standpoint of evidence preservation, however, is that this yet-to-be-identified and yet-to-be-reviewed electronic evidence is subject to varying automatic purge or overwriting processes, causing potentially relevant electronic evidence to be overwritten every day, a phenomenon that simply does not happen as rapidly, as automatically, or as invisibly with paper evidence. Even for lawyers and companies experienced with electronic evidence issues, it can be a time-consuming and expensive endeavor to understand what relevant

electronic evidence exists and to take the steps necessary to preserve that evidence. When a preservation obligation arises, parties must respond quickly and attempt to preserve the status quo – the function of the electronic evidence triage team.

I. INTRODUCTION

Given the staggering amount of electronic evidence that is daily generated, stored, transmitted – and systematically overwritten or purged – a special examination of litigation-driven evidence preservation requirements is warranted. When advising a client about electronic evidence preservation issues, Texas practitioners should be guided by this relatively straightforward proposition: “[I]f a party violates a statutory, regulatory, or ethical duty to preserve evidence, the party may be subject to either sanctions or a spoliation presumption.”¹ Just as importantly – and this is an often-overlooked fact that rarely becomes the subject of a court decision – your client's electronic evidence just might help you prove your theories of the case. Many companies create electronic evidence that would help show that they acted responsibly, made reasonable decisions, and are being wrongfully accused in the lawsuit. In any event, whether the electronic evidence helps or hurts your case, if relevant, it must be preserved.

Most decisions regarding electronic evidence *preservation*, as opposed to electronic evidence *production*, must be made before the litigant has a practical ability to seek guidance from the court or agreement of the other side. Thus, important and likely expensive electronic evidence preservation decisions must be based on a careful and fact-intensive analysis. This paper attempts to provide guidance and suggestions to those facing these electronic discovery preservation questions:

- When and how does the duty to preserve electronic evidence arise?
- What electronic evidence must be preserved?
- What steps should parties take to comply with the duty to preserve electronic evidence?
- What could happen to parties who fail to preserve electronic evidence?

The questions of “when to preserve” and “what could happen if I get it wrong” are relatively easy to answer, as the discovery rules necessary to resolve

¹ *Trevino v. Ortega*, 969 S.W.2d 950, 955 (Tex. 1998) (Baker, J., concurring).

these questions translate readily from paper evidence to electronic evidence. As for the questions of “what to preserve” and “how to comply,” there simply are no black-and-white answers. A lawyer attempting to answer these questions must combine many skills: lawyer, computer expert, detective, and perhaps most importantly, fortune teller – to predict what electronic evidence your opponent will really need (for the merits of the case) and claim it wants (for sanctions) and to predict how the judge will rule. Taking an overly conservative approach to these decisions could cost tens or hundreds of thousands of dollars and even outweigh the value of the case.² But taking an aggressive or careless approach -- or even being well-intentioned but guessing wrong -- and allowing electronic evidence to “disappear” exposes the lawyer and client to sanctions.

II. WHEN AND HOW IS THE DUTY TO PRESERVE ELECTRONIC EVIDENCE TRIGGERED?

Duties or needs to preserve electronic evidence arise in many different ways. There are statutes and regulations that govern retention of electronically stored records. There are business needs to keep electronic records. And there is a duty to preserve evidence based on actual or expected litigation. This paper will focus on litigation-driven preservation duties, but it will briefly mention the other reasons in the context of how they could affect litigation. The focus of this paper will also be from the perspective of the party with the preservation obligation, as opposed to the party seeking electronic discovery.

A. Litigation, Investigations, and Other Disputes

1. Actual or Anticipated Litigation

The most recent pronouncement by the Texas Supreme Court is that a duty to preserve evidence “arises only 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 or control

will be material and relevant to that claim.”³ The duty has also been described as follows:

A party that is on notice of either potential or pending litigation has an obligation to preserve evidence that is relevant to the litigation. “While a litigant is under no duty to keep or retain every document in its possession . . . , it is under a duty to preserve what it knows, or reasonably should know, is relevant in the action, is reasonably calculated to lead to discovery of admissible evidence, is reasonably likely to be requested during discovery, [or] is the subject of a pending discovery sanction.”⁴

This duty applies to both paper and electronic evidence.⁵ The preservation obligation is based on the totality of the circumstances and is based on an objective or subjective test: whether “the party either actually anticipated litigation *or* a reasonable person in the party’s position would have anticipated litigation.”⁶

³ *Wal-Mart Stores Inc. v. Johnson*, 106 S.W.3d 718, 722 (Tex. 2003) (citing 1 WEINSTEIN & BERGER, WEINSTEIN’S FEDERAL EVIDENCE § 301.06[4] at 301-28.3 (2d ed. 2003)).

⁴ *Trevino*, 969 S.W.2d at 957 (Baker, J., concurring) (quoting *Wm. T. Thompson Co. v. Gen. Nutrition Corp.*, 593 F. Supp. 1443, 1455 (C.D. Cal. 1984)); *see also Silvestri v. Gen. Motors Corp.*, 271 F.3d 583, 591 (4th Cir. 2001) (“The duty to preserve material evidence arises not only during litigation but also extends to that period before the litigation when a party reasonably should know that the evidence may be relevant to anticipated litigation.”) (citations omitted); *Madden v. Wyeth*, No. 3-03-CV-0167-R, 2003 WL 21443404, at *1 (N.D. Tex. Apr. 16, 2003) (“*all litigants* are obligated to take appropriate measures to preserve documents and information which are reasonably calculated to lead to the discovery of admissible evidence and likely to be requested during discovery”).

⁵ *See, e.g., Positive Software Solutions Inc. v. New Century Mortgage Corp.*, 259 F. Supp. 2d 561, 562 (N.D. Tex. 2003) (issuing preservation order for “all extant backups or images of all servers or personal computers that now or previously contained any portion or part of [software programs at issue in the case], whether used for development, debugging, deployment, production or otherwise, including source code, object code, history or log files, or revision tracking files”); *Zubulake v. UBS Warburg LLC*, No. 02 Civ. 1243(SAS), 2003 WL 22410619 (S.D.N.Y. Oct. 22, 2003) (applying duty to electronic evidence); *In re Triton Energy Ltd. Sec. Litig.*, No. 5:98CV256, 2002 WL 32114464, at *4 (E.D. Tex. Mar. 7, 2002).

⁶ *Trevino*, 969 S.W.2d at 956 (Baker, J., concurring); *Wal-Mart*, 106 S.W.2d at 722 (“knows or reasonably should know”). This test is derived from and virtually identical to “anticipation of litigation” in the context of whether a party should be allowed to assert the former “investigative

² Electronic evidence preservation efforts often carry a steep cost. For example, consider a client with 30 e-mail servers and 30 days of back-up tapes for each server. Assuming each back-up tape costs \$60, simply pulling the back-up tapes out of rotation would require the company to spend more than \$50,000 to obtain new tapes, to say nothing of the effort and money necessary to copy and change out the tapes.

Courts have applied somewhat of a sliding-scale approach to the duty to preserve evidence.⁷ At one end of the sliding scale, once a party receives a discovery request, it clearly has a duty not to destroy responsive documents.⁸ Next, once a party is served with a complaint, it has a duty to preserve evidence that, under the allegations set forth in the complaint, is relevant and reasonably likely to be the subject of a discovery request, even if no such request has actually been received.⁹ Finally, courts recognize a duty to preserve evidence simply when a party has knowledge of an incident that is likely to give rise to litigation, even when no complaint has been filed.¹⁰ Many

privilege.” See *Trevino*, 969 S.W.2d at 956 (Baker, J., concurring). The “investigative privilege” of former Tex. R. Civ. P. 166b(3)(d) protected only those communications made in connection with the “particular suit” or in anticipation of the “pending litigation,” while the “work product” privilege under new Tex. R. Civ. P. 192.5(a)(2) does not contain that limitation. See *In re Monsanto Co.*, 998 S.W.2d 917, 922 n.3 (Tex. App. – Waco 1999, no pet.).

⁷ See *Wm. T. Thompson Co. v. Gen. Nutrition Corp.*, 593 F. Supp. 1443, 1456-57 (C.D. Cal. 1984) (discussing available sanctions).

⁸ See, e.g., *Computer Assocs. Int’l Inc. v. Am. Fundware, Inc.*, 133 F.R.D. 166 (D. Colo. 1990) (imposing default judgment for failure to preserve evidence both before service of discovery request, when party should have anticipated litigation, and continuing until ruling on motion to compel production).

⁹ See *Kronisch v. United States*, 150 F.3d 112, 126 (2d Cir. 1998) (lawsuit puts parties on notice); *Electron, Inc. v. Overhead Door Corp.*, 116 F.R.D. 107, 127 (S.D. Fla. 1987) (filing of complaint that was served on and read by chief legal counsel imposed preservation obligation); *Wiginton v. Ellis*, No. 02 C6832, 2003 WL 22439865, at *4 (N.D. Ill. Oct. 27, 2003) (lawsuit put party on notice of preservation obligation, and preservation letter served to further particularize types of evidence that would be sought).

¹⁰ See *Kronisch*, 150 F.3d at 127 (sanctions appropriate where court found destruction of documents two years before suit was motivated by “fear that the documents would become the subject of litigation”); *McGinnity v. Metro-N. Commuter R.R.*, 183 F.R.D. 58, 60 (D. Conn. 1998) (“obligation to preserve evidence even arises prior to the filing of a complaint where a party is on notice that litigation is likely to be commenced”); *Century ML-Cable Corp. v. Conjugal P’ship*, 43 F. Supp. 2d 176, 181 n.8 (D.P.R. 1998) (“it is well established that a party’s obligation to preserve evidence relevant to claims against it arises at the time the party becomes aware that claims may be asserted against it”); *Howell v. Maytag*, 168 F.R.D. 502, 505 (M.D. Pa. 1996) (“party which reasonably anticipates litigation has an affirmative duty to preserve relevant evidence”) (citing *Baliois v. McNeil*, 870 F. Supp. 1285, 1290 (M.D. Pa. 1994)). The existence of a pre-litigation duty to preserve evidence is a substantive issue and thus is governed by the law of the jurisdiction in diversity actions in federal court. See *State Farm Fire & Cas. Co. v. Frigidaire*, 146 F.R.D.

factors can show that a party is on notice that a lawsuit is likely, such as the magnitude of the loss, the party’s attempts to document the damage through photographs and reports, and the quick retention of attorneys and experts.¹¹

As these cases make clear, the duty to preserve electronic evidence can originate or be defined by many events, such as the occurrence of an incident likely to give rise to a lawsuit,¹² preparing to file a lawsuit,¹³ receipt of a pre-litigation demand letter,¹⁴ receipt of a document preservation letter or preservation order,¹⁵ receipt of a lawsuit,¹⁶ notice of initiation of a government investigation,¹⁷ or receipt of a discovery request or a subpoena.¹⁸ Further, the scope

160, 162 (N.D. Ill. 1992); see also *Thomas v. Bombardier-Rotax Motorenfabrik*, 909 F. Supp. 585, 587 (N.D. Ill. 1996) (holding state law governed issue of appropriate sanction for destruction of evidence).

¹¹ See, e.g., *McGinnity*, 183 F.R.D. at 61.

¹² See *supra* nn. 3, 4; *McLain v. Taco Bell Corp.*, 527 S.E.2d 712, 718 (N.C. App. 2000); *Aggrey v. Stop & Shop Supermarket Co.*, No. 00 CIV. 7999(FM), 2002 WL 432388 (S.D.N.Y. Mar. 19, 2002).

¹³ See *Skeete v. McKinsey & Co.*, No. 91 Civ. 8093 (PKL), 1993 WL 256659 (S.D.N.Y. July 7, 1993).

¹⁴ See *Abramowitz v. Inta-Boro Acres Inc.*, No. 98-CV-4139 (ILG), 1999 WL 1288942, at *3 (E.D.N.Y. Nov 16, 1999); *Bradley v. Sunbeam Corp.*, No. 5:99CV144, 2003 WL 21982038 (N.D. W.Va. Aug. 4, 2003).

¹⁵ See, e.g., *Danis v. USN Communications, Inc.*, No. 98 C 7482, 2000 WL 1694325 (N.D. Ill. Oct. 23, 2000). Document preservation letters and preservation orders are discussed in more detail below. See *infra* § II(A)(2).

¹⁶ See *supra* nn. 3, 4; *Kronisch*, 150 F.3d at 126; *Riddle v. Liz Claiborne, Inc.*, No. 00 Civ. 1374 MBMHBP, 2003 WL 21976403 (S.D.N.Y. Aug. 19, 2003); *Aggrey*, 2002 WL 432388.

¹⁷ See *Zubulake*, 2003 WL 22410619, at *2 (filing of EEOC charge).

¹⁸ A subpoena recipient must produce all responsive material in its possession, custody, or control, unless the recipient objects or a court orders otherwise. A court can treat failure to comply as a contempt of court, even in the absence of a court order. Tex. R. Civ. P. 176.8; Fed. R. Civ. P. 45(e); see, e.g., *Fletcher v. Dorchester Mut. Ins. Co.*, 773 N.E.2d 420, 425 (Mass. 2002); *Williams v. Mercer*, 783 F.2d 1488, 1495 (11th Cir. 1986). The Texas and Federal Rules impose limits on subpoenas to non-parties. A litigant or attorney issuing a subpoena “must take reasonable steps to avoid imposing undue burden or expense” on the subpoena recipient. Tex. R. Civ. P. 176.7; Fed. R. Civ. P. 45(c)(3)(A),(B). A court must quash or modify a subpoena if it does not allow a reasonable time for compliance, requires disclosure of privileged material, or subjects the recipient to an undue burden. Tex. R. Civ. P. 176.7; Fed. R. Civ. P. 45(c)(3)(A). Also, a court has discretion to quash,

of the duty to preserve may evolve as the litigation matures. For example, new obligations may arise when third-party or counter-claims are prepared or received, when amendments to complaints or answers are filed, when new discovery requests are served, or when new witnesses, new evidence, or new arguments emerge. The converse should also be true: once-existing preservation obligations may disappear when parties are dismissed, claims are dropped, or court rulings dispose of questions relating to what is relevant in the case. Counsel must constantly evaluate how changes in a case affect preservation obligations.

2. Preservation Letters and Preservation Orders

It is becoming more common, especially with the exploding electronic discovery phenomenon, for litigants to send written preservation demands at or even before the commencement of litigation. A typical preservation letter will purport to notify its recipient of its duty to preserve both general and specific electronic evidence, and will threaten sanctions for any failure to comply with preservation demands. These letters are especially popular tactical tools with litigants who have little or no electronic evidence themselves.

Preservation obligations, of course, exist separate and apart from a preservation letter. “While a litigant certainly may request that an adversary agree to preserve electronic records during the pendency of a case, or even seek a court order directing that this happen, it is not required, and a failure to do so does not vitiate the independent obligation of an adverse party to preserve such information.”¹⁹ A preservation letter may be useful, however, in creating “notice” and delineating certain types of information that will be the subject of discovery that may not have been originally anticipated by the receiving party.²⁰

In addition to using the preservation letter strategy, some litigants have successfully convinced courts to enter electronic evidence preservation orders.²¹ Other courts have rejected the notion that

modify, or condition compliance with a subpoena if it requires disclosure of trade secrets or other confidential material. Fed. R. Civ. P. 45(c)(3)(B).

¹⁹ *Thompson v. United States Dep’t of Housing & Urban Dev.*, 219 F.R.D. 93, 100 (D. Md. 2003) (footnote omitted).

²⁰ See *Wiginton*, 2003 WL 22439865, at *4 (party receiving preservation letter has no duty to respond to or comply with letter, but letter was significant because it alerted party to type of electronic evidence likely to be requested during discovery).

²¹ See, e.g., *Newby v. Enron Corp.*, 302 F.3d 295, 299-300 (5th Cir. 2002) (discussing evidence preservation order

preservation orders should be routinely issued.²² As with preservation letters, preservation obligations exist independently of a court order.²³

3. Documents in Your Client’s “Possession, Custody, or Control”

It is not always sufficient to preserve only the evidence in your client’s physical possession. A party must produce – and therefore take steps to preserve – all responsive evidence in its “possession, custody, or control.”²⁴ Evidence is considered to be within the “possession, custody, or control” of a party if the party has actual possession, custody, or control, or the legal right to obtain the documents on demand.²⁵ Some courts have held that a party must produce requested documents if it has the “practical ability to obtain the documents from another, irrespective of his legal entitlement to the documents.”²⁶ Other courts,

covering documents related to bankrupt company and duplicative state court ex parte temporary restraining orders); *Dodge, Warren & Peters Ins. Servs., Inc. v. Riley*, 105 Cal. App. 4th 1414, 1418, 130 Cal. Rptr. 2d 385 (2003) (applying standards for preliminary injunction to request for preservation order).

²² See *Madden*, 2003 WL 21443404, at *1 (to “supplement every complaint with an order requiring compliance with the Rules of Civil Procedure would be a superfluous and wasteful task and would likely create no more incentive upon the parties than already exists”) (quoting *Hester v. Bayer Corp.* 206 F.R.D. 683, 685 (M.D. Ala. 2001)); see also *The Sedona Principles: Best Practices Recommendations & Principles for Addressing Electronic Document Production* at 12-13, available at www.sedona.org, Jan. 2004 (hereinafter “*Sedona Principles*”) (“[P]reservation orders should be issued rarely, and only in cases in which the standards for injunctive relief have been met.”).

²³ See *Thompson*, 219 F.R.D. at 99 (stating that preservation order or lack thereof does not negate independent preservation obligation).

²⁴ See Fed. R. Civ. P. 34(a); Tex. R. Civ. P. 192.3(b).

²⁵ See Tex. R. Civ. P. 192.7(b) (physical possession or right of possession equal or superior to right of person having physical possession); *In re Kuntz*, 124 S.W.3d 179, 181 (Tex. 2003); *In re Bankers Trust Co.*, 61 F.3d 465, 469 (6th Cir. 1995); *Searock v. Stripling*, 736 F.2d 650, 653 (11th Cir. 1984); *McCoo v. Denny’s Inc.*, 192 F.R.D. 675, 692 (D. Kan. 2000).

²⁶ See *Prokosch v. Catalina Lighting, Inc.*, 193 F.R.D. 633, 636 (D. Minn. 2000) (quoting *United States v. Skeddle*, 176 F.R.D. 258, 261 n.5 (N.D. Ohio 1997) (citations omitted)); *accord Bank of N.Y. v. Meridien BIAO Bank Tanzania, Ltd.*, 171 F.R.D. 135, 146 (S.D.N.Y. 1997); *Scott v. Arax, Inc.*, 124 F.R.D. 39, 41 (D. Conn. 1989).

however, have required parties to produce only those documents they have a legal right to obtain.²⁷

Courts generally hold that a parent corporation has a sufficient degree of ownership and control over a wholly-owned subsidiary such that the parent is deemed to have control over the subsidiary's documents.²⁸ This principle has been applied even when the subsidiary is not owned directly but, rather, is owned by an intermediate corporation that is itself a wholly-owned subsidiary of the parent corporation.²⁹ Documents held by a subsidiary or branch office in another state or even a foreign country have been held to be within a party's control and subject to production.³⁰

²⁷ See, e.g., *In re Kuntz*, 124 S.W.3d at 184 (employee's mere access to employer documents not "physical possession" under Tex. R. Civ. P. 192.7(b)); *Chaveriat v. Williams Pipe Line Co.*, 11 F.3d 1420, 1427 (7th Cir. 1993) ("But the fact that a party could obtain a document if it tried hard enough . . . does not mean that the document is in its possession, custody, or control"); *Bleecker v. Standard Fire Ins. Co.*, 130 F. Supp. 2d 726, 739 (E.D.N.C. 2000) (rejecting practical ability to obtain test in favor of stricter legal control test); see also *In re Citric Acid Litig.*, 191 F.3d 1090, 1107-08 (9th Cir. 1999) (adopting legal control test for Rule 45 subpoenas).

²⁸ See, e.g., *United States v. Int'l Union of Petroleum & Indus. Workers*, 870 F.2d 1450, 1452 (9th Cir. 1989) ("A corporation must produce documents possessed by a subsidiary that the parent corporation owns or wholly controls."); *Alden v. Time Warner, Inc.*, No. 94 Civ. 6109, 1995 WL 679238, at *2 (S.D.N.Y. Nov. 14, 1995) (corporate parent required to produce documents held by subsidiary); *Camden Iron & Metal, Inc. v. Marubeni Am. Corp.*, 138 F.R.D. 438, 441 (D.N.J. 1991) (parent corporation has control over documents in physical control of wholly owned or controlled subsidiary); *In re Uranium Antitrust Litig.*, 480 F. Supp. 1138, 1152 (N.D. Ill. 1979) (corporate parent must produce documents of wholly owned subsidiary but not documents of 43.8%-owned subsidiary that conducted its corporate affairs separately); *Hubbard v. Rubbermaid, Inc.*, 78 F.R.D. 631, 637 (D. Md. 1978) (parent corporation must produce documents held by wholly owned subsidiaries, and fact that subsidiaries were separate corporate entities was irrelevant).

²⁹ See *Lethbridge v. British Aerospace PLC*, No. 89 Civ. 1407, 1990 WL 194915, at *1 (S.D.N.Y. Nov. 28, 1990).

³⁰ See *In re Uranium*, 480 F. Supp. at 1144-53 (holding that location of documents is irrelevant and granting motions to compel some defendants to produce foreign documents); *Gerling Int'l Ins. Co. v. Comm'r*, 839 F.2d 131, 140 (3d Cir. 1988) ("the location of the documents is . . . irrelevant"); *McKesson Corp. v. Islamic Republic of Iran*, 185 F.R.D. 70, 78 (D.D.C. 1999) (requiring production because foreign entity was agent of Iran and stating that "[t]he control analysis for Rule 34 purposes does not require the party to have actual managerial power over the foreign corporation, but rather that there be a close coordination between them") (citing *Afros S.P.A. v. Krauss-Maffei Corp.*, 113 F.R.D. 127,

These cases make clear that litigants need to ask – and answer – this question: Who has (or where is) the electronic evidence relating to this case? Relevant electronic evidence is frequently not in the physical possession of the litigants. Companies often outsource functions that in the past were handled internally, e.g., payroll, billing, customer call center, and manufacturing. Electronic evidence may also exist in the physical possession of parent, subsidiary, or affiliated companies, or with partners or joint venturers, current or former directors, officers, employees, or consultants, and any number of other third parties over whom the litigant may be deemed to have "possession, custody, or control."³¹ The litigant, therefore, must take steps to ensure that third parties having custody of relevant electronic evidence are informed of the preservation obligation.³² A litigant may also have a duty to inform its opponent of evidence it does not control: "If a party cannot fulfill this duty to preserve because he does not own or control the evidence, he still has an obligation to give the opposing party notice of access to the evidence or of the possible destruction of the evidence if the party anticipates litigation involving that evidence."³³

B. Statutory and Regulatory Obligations

There are thousands of statutes and regulations that deal with the retention of business documents, and they vary by industry, corporate structure, and/or the nature and content of the record. These obligations arise independently of any threatened or pending litigation. As noted above, statutory and regulatory retention requirements are beyond the scope of this

129 (D. Del. 1986)); *Johnson v. Cloos Int'l, Inc.*, No. 89 C8483, 1990 WL 106560, at *1-2 (N.D. Ill. July 11, 1990) (ordering production of documents of foreign parent); *Cooper Indus., Inc. v. British Aerospace, Inc.*, 102 F.R.D. 918, 919-20 (S.D.N.Y. 1984) (ordering production of documents in possession of foreign affiliates).

³¹ See, e.g., *In re Triton*, 2002 WL 32114464, at *4, 6 ("it would have been prudent and within the spirit of the law for Triton to instruct its [outside directors] to preserve and produce any documents in their possession, custody, or control," even though they were not Triton employees).

³² See, e.g., *Keir v. UnumProvident Corp.*, No. 02 Civ. 8781(DLC), 2003 WL 21997747, at *7, 12 (S.D.N.Y. Aug. 22, 2003) (finding that defendant failed to communicate in a timely manner preservation obligation to third-party provider of e-mail and other computer services).

³³ See *Silvestri*, 271 F.3d at 591 (plaintiff injured in automobile accident should have given defendant manufacturer notice and equal access to vehicle before vehicle was destroyed, even though plaintiff did not own vehicle).

paper with one exception: The failure of a litigant to comply with its statutory or regulatory electronic evidence preservation obligations could be used by an opponent to support a sanctions motion.³⁴

C. Business Needs

Independent of statutory or regulatory retention requirements, companies of course have their own business needs for keeping electronic information. Due to these needs, many businesses have adopted document retention policies and procedures.³⁵ As with a failure to abide by statutory preservation obligations, the failure of a litigant to abide by its own retention guidelines could be used by its opponent to support a sanctions motion.³⁶

III. WHAT ELECTRONIC EVIDENCE MUST BE PRESERVED?

Once the obligation to preserve evidence is triggered, the next question that arises is what electronic evidence needs to be preserved. To answer the “what” question requires some of the steps a lawyer would take if dealing with paper records (e.g., determining what type of evidence is relevant to the

³⁴ See *Park v. City of Chicago*, 297 F.3d 606, 615 (7th Cir. 2002) (bad faith violation of record retention regulation may result in adverse inference); *Byrnie v. Town of Cromwell Bd. of Educ.*, 243 F.3d 93, 108-09 (2d Cir. 2001) (“Several courts have held that destruction of evidence in violation of a regulation that requires its retention can give rise to an inference of spoliation.”); see also *Trevino*, 969 S.W.2d at 955 (Baker, J., concurring) (citing cases where statutes imposed a duty to maintain medical records).

³⁵ See Sedona Principles at 12-13.

³⁶ See *Brown & Williamson Tobacco Corp. v. Jacobson*, 827 F.2d 1119, 1135 (7th Cir. 1987) (employee’s destruction of documents in violation of employer’s retention policy was evidence of bad faith). Further, courts recognize that at least minimal documentation must be retained for business purposes. In *Kucala Enterprises, Ltd. v. Auto Wax Co.*, No. 02 C 1403, 2003 WL 21230605, at *6 (N.D. Ill. May 27, 2003), the court stated that it was “not persuaded that the normal course of one’s business is to delete business correspondence, e-mails, and invoices. . . . [T]he Court is stunned that a person can run a business without keeping customer files that would include letters and invoices.” The belief that certain documentation should have been retained for a business need, along with other factors, led the court to conclude that there had been willful destruction of potentially relevant evidence and to dismissal of the case. *Id.* at *8; see also *In re Dynamic Health, Inc.*, 32 S.W.3d 876, 885 (Tex. App. – Texarkana 2000, pet. denied) (“A large medical facility would normally have records of the origin, age, and description of the personal property contained within its facility, if only for insurance and tax purposes.”).

case based on factual allegations, legal theories, and an understanding of the client’s business), but other steps that typically are not part of paper discovery (e.g., interviewing IT and related operations personnel, mapping IT infrastructure, gathering database file layouts, reviewing purge processes, and exploring the company’s archiving or tape library). In assessing what electronic evidence to preserve, it is first useful to highlight some of the differences between paper and electronic evidence.

A. Key Differences Between Paper Documents and Electronic Evidence

First, electronic evidence cannot easily be touched, seen, or quantified. Paper evidence, by contrast, can be held, stacked, flagged, highlighted, separated into relevant and not relevant, spread out on a conference room table and compared side-by-side, copied, boxed, and shipped. Electronic evidence is plainly different, in that it must typically be viewed and handled through a piece of hardware, like a computer monitor. And while the monitor may allow a reviewer to see files, applications, and particular data, there are other components of electronic evidence that cannot easily be seen – or even found other than by a true computer expert – on a computer monitor. In essence, all lawyers know how to review a file, a box, or a room full of paper. But when faced with a hard drive or a network of computers, applications, and databases to review, few lawyers can locate, much less work with, this electronic evidence without considerable technical assistance.

Second, the term “electronic evidence” can include massive amounts of information. “For example, the scope of what is included in the phrase ‘electronic records’ can be enormous, encompassing voice mail, e-mail, deleted e-mail, data files, program files, back-up files, archival tapes, temporary files, system history files, web site information in textual, graphical or audio format, web site files, cache files, ‘cookies’ and other electronically stored information.”³⁷ A single hard drive may contain the equivalent of millions of pages of paper.

Third, unlike paper documents, many electronic documents and collections are never fixed in a final form.³⁸ For example, back-up tapes are overwritten, web pages are updated, and e-mail systems may

³⁷ *Thompson*, 219 F.R.D. at 96; see also Sedona Principles at 3-4 (noting volume and duplicability as some of the main differences between electronic documents and paper documents).

³⁸ See Sedona Principles at 4.

reorganize and remove data automatically.³⁹ Also, electronic evidence is more easily modified. For example, merely moving a word processing file from one location to another can change creation or modification dates.⁴⁰

Fourth, “deleted” electronic evidence may still be recoverable, and some courts have held that such evidence is discoverable.⁴¹ “Deleted” evidence may be automatically overwritten, however, unless it is immediately recovered, a process that can be very time-consuming and expensive.⁴²

Finally, electronic evidence contains “metadata,” or certain data (which may be hidden or embedded) that describes the content, quality, condition, history, and other characteristics of the document or file.⁴³ Metadata can be useful to show inadvertent or deliberate modification of the evidence or the authenticity of a document, and it can be preserved without additional costs or steps when electronic evidence is preserved in its native format.⁴⁴

B. All Relevant, Non-Duplicative Electronic Evidence Should Be Preserved

The basic rule is that evidence is discoverable if it is relevant to the claims or defenses in the case.⁴⁵ The rule is not different for electronic evidence. Therefore, if electronic evidence is discoverable, it should be preserved.⁴⁶ Courts have held that a “party does not have to go to extraordinary measures to preserve all potential evidence.”⁴⁷ But those cases do not excuse

preservation of all relevant electronic evidence. Rather, they are based on the notion that the evidence excused from production was not unique or not relevant.⁴⁸

Texas has created a presumption that heroic efforts to *produce* electronic evidence are not required, at least not on the producing party’s nickel. Under the Texas Rules, the responding party is required to:

produce the electronic or magnetic data that is responsive to the request and *is reasonably available to the responding party in its ordinary course of business*. If the responding party cannot – through reasonable efforts – retrieve the data or information requested or produce it in the form requested, the responding party must state an objection complying with these rules.⁴⁹

But litigants should not necessarily rely on the “reasonably available in the ordinary course” *production* standard when making decisions about *preservation*. Indeed, the rule provides for cost-shifting when a court orders production of electronic evidence that cannot be produced through reasonable efforts.⁵⁰ Thus, this rule suggests that, even when relevant and responsive electronic evidence cannot be produced through reasonable efforts, that evidence should nonetheless be preserved pending resolution by a court.

C. Electronic Evidence That May Not Have To Be Preserved

Some courts have suggested that specific types of electronic evidence – back-up tapes, deleted data, and electronic evidence that is duplicative of paper evidence – may not be subject to a preservation obligation in the ordinary case. But the law is sparse in this area, and counsel cannot take for granted that they

necessary to freeze all electronic documents and data, just as it is not necessary to preserve contents of waste baskets to preserve paper evidence; “there should be a similar application of reasonableness to preservation of electronic documents and data”).

⁴⁸ See *Wiginton*, 2003 WL 22439865, at *4 (“But a party must preserve evidence that it has notice is reasonably likely to be the subject of a discovery request”); see also *Zubulake*, 2003 WL 22410619, at *3 (“At the same time, anyone who anticipates being a party or is a party to a lawsuit must not destroy unique, relevant evidence that might be useful to an adversary.”).

⁴⁹ Tex. R. Civ. P. 196.4 (emphasis added).

⁵⁰ *Id.*

³⁹ *See id.*

⁴⁰ *See id.*

⁴¹ *See infra* § III(C)(2).

⁴² *See* Sedona Principles at 4 (electronic documents more difficult to dispose of than paper documents).

⁴³ *See id.* at 4-5.

⁴⁴ *Id.*; *cf. id.* at 41 (while metadata should be presumptively irrelevant, “particular metadata may be critical” depending on the circumstances of the case).

⁴⁵ Fed. R. Civ. P. 26(b)(1). If good cause is shown, the court may expand the scope of discovery to any matter relevant to the subject matter of the action. *Id.*; compare Tex. R. Civ. P. 192.3(a) (evidence is discoverable if “relevant to the subject matter of the pending action, whether it relates to the claim or defense of the party seeking discovery or the claim or defense of any other party”).

⁴⁶ *See Wiginton*, 2003 WL 22439865, at *4; see also *supra* § II(A) (discussing preservation duty generally).

⁴⁷ *Wiginton*, 2003 WL 22439865, at *4 (citation omitted); see also *Zubulake*, 2003 WL 22410619, at *3 (a corporation does not have to preserve “every shred of paper, every e-mail or electronic document, and every backup tape”); Sedona Principles at 24 (stating that it is not

will be the beneficiaries of similar rulings. Indeed, when courts have determined that certain types of electronic evidence need not be produced, they typically have done so because the data was assumed to exist in another, more accessible location. Even these courts recognized that a litigant should not destroy unique, relevant data.⁵¹

1. Back-Up Tapes

Back-up tapes may be discoverable and therefore subject to preservation obligations.⁵² Some courts, however, have held that back-up tapes created in the ordinary course of business and maintained for disaster recovery were “inaccessible” and, as a general rule, not subject to preservation obligations:

Once a party reasonably anticipates litigation, it must suspend its routine document retention/destruction policy and put in place a ‘litigation hold’ to ensure the preservation of relevant documents. As a general rule, that litigation hold does not apply to inaccessible back-up tapes (*e.g.*, those typically maintained solely for the purpose of disaster recovery), which may continue to be recycled on the schedule set forth in the company’s policy. On the other hand, if back-up tapes are accessible (*i.e.*, actively used for information retrieval), then such tapes would likely be subject to the litigation hold.⁵³

⁵¹ See *Zubulake*, 2003 WL 22410619, at *3 (“[A]nyone who anticipates being a party or is a party to a lawsuit must not destroy unique, relevant evidence that might be useful to an adversary.”); see also Sedona Principles at 23 (if there is substantial likelihood that relevant information exists in that normally-unproducible form and would otherwise, absent intervention, not remain in existence, steps should be taken to preserve evidence anyway).

⁵² See *Wiginton*, 2003 WL 22439865 (discussing destruction of back-up tapes that should have been preserved); *Landmark Legal Found. v. Env’tl. Protection Agency*, 272 F. Supp. 2d 70 (D.D.C. 2003) (same); *In re CI Host, Inc.*, 92 S.W.3d 514 (Tex. 2002) (upholding order to produce back-up tapes); *Renda Marine, Inc. v. United States*, 58 Fed. Ct. 57 (Fed. Cl. 2003) (ordering production of back-up tapes); *Medtronic Sofamor Danek, Inc. v. Michelson*, No. 01-2373-MIV, 2003 U.S. Dist. LEXIS 8587, at *8 (W.D. Tenn. May 13, 2003) (acknowledging discoverability of back-up tapes).

⁵³ *Thompson*, 219 F.R.D. at 100 (quoting *Zubulake*, 2003 WL 22410619, at *4); see *McPeck v. Ashcroft*, 202 F.R.D. 31, 32-33 (D.D.C. 2001) (noting lack of authority for requiring restoration of all back-up tapes in every case and explaining the “purpose of having a backup system and retaining the tapes” can be “to permit recovery from a

This general rule would not apply if the information on the back-up tapes was not otherwise available.⁵⁴ Whether ultimately *producible* or not, the decision on whether to *preserve* back-up tapes must usually be made early in the litigation and often without the benefit of a court’s decision. Therefore, as discussed below, it may be prudent to identify back-up tapes to contain discoverable electronic evidence and remove them from service pending agreement of the parties or a court ruling.

2. “Deleted” Electronic Evidence

Electronic evidence is often preserved inadvertently. Instead of being erased when a user marks files for deletion, electronic files marked for deletion are designated as unused disk space that may be overwritten – something that may occur shortly after “deletion” or may never occur. Under the right circumstances, courts allow discovery of “deleted”

disaster, not archival preservation”); see also Sedona Principles at 24 (“Absent specific circumstances, preservation obligations should not extend to disaster recovery backup tapes created in the ordinary course of business.”).

⁵⁴ See, *e.g.*, *Zubulake*, 2003 WL 22410619, at *4 (“If a company can identify where particular employee documents are stored on backup tapes, then the tapes storing the documents of “key players” to the existing or threatened litigation should be preserved if the information contained on those tapes is not otherwise available.”).

electronic records.⁵⁵ As with back-up tapes, however, the decision on whether to preserve deleted electronic evidence may need to be made well before the court will resolve whether the deleted electronic evidence must be produced.

3. Duplicative Paper and Electronic Evidence

Some courts have held that a party need not produce electronic evidence when it has already produced paper copies of that evidence.⁵⁶ But most cases hold that producing paper records will not relieve a party of producing the electronic versions of those same documents.⁵⁷ If it can be determined that the

⁵⁵ See *Thompson*, 219 F.R.D. at 97 (citing multiple court decisions holding that deleted computer records are discoverable); *Zubulake v. UBS Warburg, LLC*, 217 F.R.D. 309, 316-17 (S.D.N.Y. 2003) (discovery is allowed of electronic records that are currently in use and that “may have been deleted and now reside only on backup disks”); *Antioch Co. v. Scrapbook Borders, Inc.*, 210 F.R.D. 645, 652 (D. Minn. 2002) (“[I]t is a well accepted proposition that deleted computer files . . . are discoverable.”); *Simon Prop. Group, L.P. v. mySimon, Inc.*, 194 F.R.D. 639, 640 (S.D. Ind. 2000) (“Computer records, including records that have been ‘deleted,’ are documents discoverable under Fed. R. Civ. P. 34”); *Gates Rubber Co. v. Bando Chem. Indus. Ltd.*, 167 F.R.D. 90, 113, 118 (D. Colo. 1996) (referring to deleted files that were recovered in discovery); see also *Zubulake*, 217 F.R.D. at 317-20 (erased, fragmented, or damaged data is “inaccessible” and therefore subject to possible cost shifting for production). But see *Sedona Principles* at 26 n.1 (“[A] party does not ordinarily have a duty to take steps to try to restore electronic information that has been deleted or discarded in the regular course of business.”) (quoting ABA Civil Discovery Standards, Standard 29(a) (iii) (1999)); *id.* at 34 (“Absent specific circumstances, organizations should not have to preserve deleted or residual data. While most computer systems will have a plethora of data that could be ‘mined,’ there should not be routine authorization for such forensic discovery. If, as usual, deleted and residual data are not accessed by employees in the ordinary course of business, there is no reason to require the routine preservation of such data.”).

⁵⁶ See *Williams v. Owens-Ill.*, 665 F.2d 918, 932-33 (9th Cir. 1982) (district court did not abuse its discretion in refusing to order production of computer tapes where requesting party already had information from the tapes on wage cards); see also *McNally Tunneling Corp. v. City of Evanston*, No. 00-C-6979, 2001 WL 1568879, at *4 (N.D. Ill. Dec. 10, 2001) (observing “apparent split of authority on whether a party is entitled to both hard-copy and electronic versions of computer files” and holding that the requesting party had failed to demonstrate that it was entitled to both).

⁵⁷ *In re Honeywell Int’l Inc. Sec. Litig.*, No. M8-85, 2003 U.S. Dist. LEXIS 20602, at *4-5 (S.D.N.Y. Nov. 18, 2003) (requiring non-party to produce electronic version of audit workpapers because they were maintained in usual course of business in electronic, not paper, form; rejecting requesting party’s request for all communications, including

relevant electronic evidence on one disk, tape, or other media is identical to other electronic evidence, a party should not need to preserve multiple identical copies of electronic evidence (for instance, multiple identical back-up tapes covering the same period).⁵⁸

IV. WHAT STEPS SHOULD BE TAKEN TO COMPLY WITH THE DUTY TO PRESERVE ELECTRONIC EVIDENCE?

The electronic evidence triage team has one overriding objective – preserve the status quo pending agreement or court resolution of preservation or production obligations.⁵⁹ This is much easier said than

e-mail, between non-party and defendant because even though non-party had produced the documents in paper form, request as framed was overly broad and had no limitation as to subject matter or individual); *Anti-Monopoly, Inc. v. Hasbro, Inc.*, No. 94CIV.2120, 1995 WL 649934, at *2 (S.D.N.Y. Nov. 3, 1995) (“The law is clear that data in computerized form is discoverable even if paper ‘hard copies’ of the information have been produced, and that the producing party can be required to design a computer program to extract the data from its computerized business records, subject to the Court’s discretion as to the allocation of the costs of designing such a computer program.”); *Anti-Monopoly, Inc. v. Hasbro, Inc.*, No. 94 Civ. 2120(LMM)(AJP), 1996 WL 22976, at *1 (S.D.N.Y. Jan. 23, 1996) (electronic data is discoverable even if paper copies have been produced). See also *Armstrong v. Executive Ofc. of the President*, 1 F.3d 1274, 1283 (D.C. Cir. 1993) (paper versions of electronic materials rarely are identical and therefore the records preservation rules for electronic materials continue to apply), *rev’d on other grounds*, 90 F.3d 553 (D.C. Cir. 1996); *Public Citizen v. Carlin*, 2 F. Supp. 2d 1, 13-14 (D.D.C. 1997) (“While an exact duplicate of a particular record might be discardable, electronic versions of records cannot categorically be regarded as valueless ‘extra copies’ of paper versions. Simply put, electronic communications are rarely identical to their paper counterparts; they are records unique and distinct from printed versions of the same record.”) (citations omitted), *rev’d on other grounds*, 184 F.3d 900 (D.C. Cir. 1999).

⁵⁸ See *Zubulake*, 2003 WL 22410619, at *4 (“A party or anticipated party must retain all relevant documents (but not multiple identical copies) in existence at the time the duty to preserve attaches, and any relevant documents created thereafter.”).

⁵⁹ It is beyond the scope of this “triage team” paper to offer suggestions on planning ahead for electronic discovery. Rather, this paper focuses on what to do to preserve the status quo once the preservation duty is triggered by litigation. But advance planning for electronic discovery is essential for most companies, as it can ease the cost, disruption, and risk of failure that comes with electronic discovery obligations.

There are many publications devoted to electronic discovery advance planning and some of the steps that may be wise to implement, such as developing e-mail retention

done. Electronic evidence is constantly being overwritten, computer systems become obsolete and unusable, and magnetic storage media deteriorates or becomes corrupted. It is well known that parties “may have relevant information, on their computer equipment, which is being lost through normal use of the computer”⁶⁰ The steps a litigant should take to preserve electronic evidence will vary from case to case. There is no one-size-fits-all approach. As a general matter, however, to preserve the status quo, litigants should assemble their electronic evidence triage team and take prompt action to learn the case and the client’s computer systems, suspend relevant electronic evidence destruction practices and issue preservation directives, and communicate with opposing counsel and the court. Litigants should also carefully document all steps taken to preserve electronic evidence.

A. Assemble The Electronic Evidence Triage Team

It is critical to assemble the right electronic evidence triage team, which will normally consist of legal, technical, and business experts. First, in-house and outside counsel must work together and direct the team. The team should also include representatives of the client’s IT department and the relevant business or operations functions (e.g., HR, operations, engineering, finance). The team may also include personnel involved in corporate document retention, compliance, and internal audit. Finally, depending on the scope of the case, the sophistication and commitment of the

policies, implementing e-mail training for employees, etc. See, e.g., Christopher V. Cotton, *Document Retention Programs for Electronic Records: Applying a Reasonableness Standard to the Electronic Era*, 24 Iowa J. Corp. L. 417 (Winter 1999); Devin Murphy, *Electronic Commerce In The 21st Century: The Discovery Of Electronic Data In Litigation: What Practitioners And Their Clients Need To Know*, 27 Wm. Mitchell L. Rev. 1825 (2001); Carey Sirota Meyer & Kari L. Wraspir, *E-Discovery: Preparing Clients for (and Protecting Them Against) Discovery In The Electronic Information Age*, 26 Wm. Mitchell L. Rev. 939 (2000); Jason Krause, *Document Management, Frequent Filers: It Takes A Policy, Computer Programs to Make Document Retention Work*, 89 ABA Journal 52 (Aug. 2003); Scott Nagel, *Automating Templates; Develop An Electronic Document Retention Policy*, 28 Law Practice Management 40 (Sept. 2002); *A Records Retention Policy in the Electronic Era*, 18 The Corporate Counsellor 1 (Jan. 2004); Andrew Dumas, *Managing Electronic Records; to Cope With Discovery, Design a Formal Record-Retention Policy and Apply it Consistently*, Legal Times 28 (Dec. 2003).

⁶⁰ *Antioch*, 210 F.R.D. at 652.

client to the process, and the level of technical skill of counsel, it is often beneficial to hire third-party technical consultants who specialize in electronic evidence litigation support.

B. Take Prompt Action

Parties should act promptly to preserve relevant electronic evidence.⁶¹ Time is of the essence in many electronic discovery cases because data is constantly being overwritten as a routine business practice.⁶² Indeed, “[d]ue to the dynamic nature of electronic data, delay in taking preservation steps may increase the danger of claims that evidence was not preserved.”⁶³ Prompt action is particularly important in cases focusing on specific conduct rather than customary practices, which often can be examined in a broader time frame.⁶⁴ And, as a practical matter, the need for immediate action may depend on the recovery of the allegations in the threatened or pending litigation. For example, if the allegations are quite recent, there is a greater danger that relevant evidence – such as voice mail or e-mail – will be automatically overwritten, as the retention period for that evidence is often just days or weeks. By contrast, there is less risk of losing relevant evidence (that has not already been lost) if the allegations are many years or even decades old.

C. Identify Relevant Electronic Evidence

As with any piece of litigation, counsel must learn the case and the client, especially the client’s computer systems. The only realistic way to identify relevant electronic evidence is to ask questions, review documents, perform computer searches, and follow the electronic “rabbit trails” that will likely be encountered. There are no magic buttons to push, and there are no reliable short cuts.

1. Learn Your Case

⁶¹ See *Keir*, 2003 WL 21997747, at *12 (“It was, therefore, incumbent on the defendants to act promptly to preserve as much as possible.”).

⁶² See *Keir*, 2003 WL 21997747 (discussing data lost though ordinary business practice due to delay in implementing retention directive); *Armstrong v. Executive Ofc. of the President*, 877 F. Supp. 750, 753 (D.D.C. 1995) (discussing overwriting of back-up tapes that occurred in course of business during lapse between temporary restraining order and permanent injunction).

⁶³ Sedona Principles at 21; see also *Keir*, 2003 WL 21997747.

⁶⁴ See *Keir*, 2003 WL 21997747, at *11.

Suggesting that counsel “learn the case” is not meant to insult anyone’s intelligence. Remember, the duty to preserve is broad, as it applies to any electronic evidence that may be relevant or that is reasonably likely to be requested during discovery.⁶⁵ So the triage team needs to learn the case from the standpoint of electronic evidence preservation. Does the case relate to company activities that are likely recorded in electronic form? Does the case involve employees or third parties who may have communicated by e-mail or voice mail? Is there a reference to a specific contract, letter, or document? Are particular company policies or practices at issue? Will there be disagreement as to whether a particular person was at a particular place at a particular time? Is it apparent that non-parties with whom your client has a relationship may be implicated? When initially approaching an electronic evidence preservation project, counsel should consider making a list of every person, company, communication, document, and incident listed in the complaint. This will provide a checklist to use as a starting point for asking about the existence of relevant electronic evidence.

Next, look at the case from the standpoint of what your opponent may consider to be relevant, even if not clearly set out in the demand letter or complaint. Is it a case about customer records, misrepresentations during the negotiation of a contract, failure to pay overtime, unauthorized access to a building, theft of trade secrets, or negligent design of a product? Ask yourself: knowing everything that I know about my client – but which my opponent may not yet know – what electronic evidence would I request in production? Obviously, if your opponent has served written discovery or sent a preservation letter, the triage team should promptly dissect the request to determine what the other side considers important and discoverable. It may also be helpful to research whether opposing counsel or the opposing litigant have any history of pursuing or resisting production of electronic evidence in other cases.

Lastly, it is also useful to look at the case from the standpoint of what discovery your opponent may do to explore your client’s computer systems and the electronic evidence preservation decisions made at the beginning of the case. Will your opponent serve interrogatories asking your client to describe its back-up tape rotation or asking you to describe all actions taken to preserve electronic evidence? Will your opponent seek production of file layouts for all databases that contain information relating to the sales of the product at issue in the case? During depositions,

⁶⁵ See *supra* § II(A)(1).

will your opponent ask your witnesses about their use of office computers, home computers, and PDAs, and will your opponent ask these witnesses whether they were notified of their duty to preserve the evidence on those computers? These types of questions will help counsel focus on the case from the standpoint of electronic evidence preservation.

2. Learn Your Client, Its Business, And The Key Personnel

This is another point that is not meant to insult anyone, but the triage team needs to learn the client, the client’s business, and the client’s key personnel in the context of preserving electronic evidence.

First, the team must understand the physical location of relevant client operations. Is the client in a single facility with no subsidiaries or affiliates, or is the client in dozens of facilities all over the world with a web of affiliates and subsidiaries? Has the client experienced any acquisitions or divestitures during the relevant time period, which may mean that relevant electronic evidence is not directly in your client’s control? Does the client handle all of its own computer functions, or does it use third parties to handle some of these functions?

Second, once the triage team understands the structure of the client, the team must learn the client’s relevant business. What were the relevant business decisions and how and why were they made? How were those decisions communicated within the company? How does information flow within the company? What reports are generated and who receives them? What are the company’s policies and procedures, and how are they implemented, tracked, measured, and audited? Have the relevant business practices changed during the time period relevant to the case, and if so, how?

Finally, the team must identify the key players in the litigation.⁶⁶ How do these employees use computers? What are the lines of communication – both up and down the corporate ladder – for these people? Are some of these key players no longer with the company (and if so, where are their computers), or are some of these employees not likely to be employed with the company for the duration of the litigation (and if so, what should you do with their computers)?

3. Learn Your Client’s Computer Systems And IT Personnel

⁶⁶ See *Thompson*, 219 F.R.D. at 1000 (electronic evidence generated or maintained by key players should be preserved); *Zubulake*, 2003 WL 22410619, at *3.

For most lawyers, learning the client's computer systems is the most challenging aspect of electronic discovery. Most lawyers do not have a computer background, and most do not care to develop this expertise. The investigation into the computer systems is where lawyers need to depend on the computer experts on the triage team.

The triage team needs to identify all relevant electronic evidence. Therefore, depending on the allegations in the case, the team may need to develop an understanding of some aspects of the client's overall system, data retention and destruction protocols, electronic back-up processes, system security, internet and e-mail systems, databases and data tables, telephone and voice mail systems, and any number of other aspects of the company's computer operations. The team may need to review system architecture layouts, database file layouts, programming or application language, purge commands, and other technical aspects of the system.

Attached at Appendix B is a generic list of topics and questions that may be a useful starting point for the triage team's investigation. One caveat before leaving this topic, however: lawyers are from Mars and computer experts are from Venus, or vice versa. Lawyers and computer experts frequently do not communicate well with each other, and assumptions about communication that lawyers have may not be the same assumptions that computer experts have. Thus, counsel must be diligent and pursue both general and specific questions in their interaction with computer experts, not unlike taking the deposition of an opposing witness. There are two good rules of thumb. First, *never* ask the question of only one member of the IT department, and *never* ask a member of the IT department the same question only once. Second, ask the computer expert to prove -- with system documentation, network searches, or any other appropriate means -- that what counsel is being told is complete and accurate. Bridging the communication gap between counsel and IT is critical to this exercise.

4. Learn Your Client's Litigation History

Most large companies have been sued hundreds or thousands of times. If other litigation resulted in preservation of electronic evidence that is not otherwise available, e.g., e-mail server back-up tapes were retained for a government investigation, counsel needs to be mindful of the fact that this evidence exists and may be relevant to other cases.⁶⁷

⁶⁷ See *Poole v. Textron, Inc.*, 192 F.R.D. 494, 502 (D. Md. 2000) (noting that defense counsel contacted prior

D. Communicate Early and Often With Opposing Counsel and Court

As noted above, many electronic evidence preservation decisions must be made early in the litigation, before the litigant has the opportunity to seek guidance from the court or opposing counsel. Further, many litigants hesitate to raise electronic discovery issues with the other side for fear that doing so would result in discovery that might not otherwise occur. Unless the electronic evidence issues in a particular case are trivial or the client does not mind devoting the money and other resources to an expensive, all-out preservation effort that still may not eliminate the possibility that the other side will discover some alleged flaw in the preservation effort, the triage team should raise electronic evidence preservation and production issues early in the case.⁶⁸ The Rule 26(f) conference is an ideal time to have these discussions if they have not already occurred, and several jurisdictions have expressly mandated that such conferences include discussion about electronic discovery.⁶⁹

Ideally, the litigants would exchange information and negotiate an agreed order on the scope of electronic evidence to be preserved and produced, which would allow the parties to resume or continue normal purging or overwriting processes for all other electronic evidence.⁷⁰ Depending on the circumstances, a litigant who wishes to have these issues resolved must be proactive and must be prepared to allow the other side formal or informal discovery into the nature and extent of available electronic evidence. The litigant may be asked to provide system or database file layouts, exemplar data, purge routines, and other documentary information necessary to allow the other side to make an informed decision on the preservation and production agreement. The litigant

outside counsel for documents from prior lawsuit, but only after suggestion from plaintiff's counsel).

⁶⁸ See Sedona Principles at 10 ("Parties should confer early in discovery regarding the preservation and production of electronic data and documents when these matters are at issue in the litigation, and seek to agree on the scope of each party's rights and responsibilities.").

⁶⁹ See U.S. DIST. CT. E.D. ARK. L. R. 26.1; U.S. DIST. CT. W.D. ARK. L. R. 26.1; U.S. DIST. CT. WYO. L. R. 26.1(d)(3)(6); and U.S. DIST. CT. N.J. L. R. 26.1(d).

⁷⁰ Sedona Principles at 16 ("By early discussion of issues such as which computer systems will be subject to preservation and discovery, the relevant time period, and the identities of particular individuals likely to have relevant electronic documents, litigants can identify and attempt to resolve disputes before they create collateral litigation.").

may also need to offer informal meetings, conference calls, or Rule 30(b)(6) depositions of IT personnel. If the parties cannot agree, it may be necessary to bring the issue to the court for resolution.

E. Suspend Relevant Electronic Evidence Destruction Activities

The triage team should identify and suspend relevant electronic evidence destruction activities.⁷¹ Companies often follow written records management policies that provide for periodic purging or overwriting of electronic evidence. In addition, whether the subject of a records management policy or not, companies have on-going, regular-course-of-business overwriting of electronic information that is no longer needed for business reasons. Finally, a litigant should determine whether other routine business functions are endangering electronic evidence that should be retained. For example, when employees leave the company, are their hard drives reformatted – thus overwriting evidence – so the computer can be used by a new employee? Does the company use data compression, disk defragmentation, or optimization programs? Do users delete temporary internet files, browser histories, and cookies? Are users able to download large files, such as .mpeg, .mp3, or .jpeg that could overwrite relevant data?

As part of this step, the triage team should collect relevant back-up tapes and image relevant hard drives.⁷² The team should also gather diskettes, Zip disks, DVDs, and similar media from key personnel.

⁷¹ See *Trevino*, 969 S.W.2d at 957 (Baker, J., concurring) (“Importantly though, when a party’s duty to preserve evidence arises before the destruction or when a policy is at odds with a duty to maintain records, the policy will not excuse the obligation to preserve evidence.”); *Wiginton*, 2003 WL 22439865, at *7 (“First, whether the documents were destroyed according to regular document retention procedures has been used as a factor to determine the reason for the destruction of documents. . . . However, once a party is on notice that specific relevant documents are scheduled to be destroyed according to a routine document retention policy, and the party does not act to prevent that destruction, at some point it has crossed the line between negligence and bad faith.”) (citation omitted); *but see Doe v. Mobile Video Tapes, Inc.*, 43 S.W.3d 40, 55-56 (Tex. App. – Corpus Christi 2001, no pet.) (no spoliation presumption regarding destroyed video evidence where television station routinely reused videotapes in ordinary course of business).

⁷² The actual mechanics of duplicating back-up tapes or imaging hard drives are beyond the scope of this memo. Typically, however, electronic evidence should be preserved with a special process that creates a mirror – or bit stream – image of the data. Relying on individual employees to keep electronic evidence may result in some employees saving too much, and other employees not saving enough. To

F. Issue Preservation Directive Governing Electronic Evidence And Related Paper Documentation

Whatever the electronic evidence triage team’s decision (or court order) regarding preservation of electronic evidence, a written document retention directive should be prepared and distributed to the appropriate personnel. This directive should cover both the electronic evidence and any related paper documentation, such as user manuals, memoranda regarding the electronic evidence or systems at issue, system diagrams, purge schedules, etc. Based on cases explaining where parties went wrong, some principles emerge that can guide parties in creating and implementing the strongest possible preservation directive.⁷³

First, an effective means of retention and compliance must be established immediately and effectively communicated to all employees that are in contact with potentially discoverable electronic evidence.⁷⁴ Do not assume that normal corporate communication practices are adequate.⁷⁵ With regard to electronic evidence, the retention directive will often have two separate audiences – IT personnel and non-IT personnel. Due to the nature of electronic evidence retention, it may be helpful to send different retention directives to the different groups, one with technical specifications to the IT employees and one with more general direction (i.e., do not delete or alter e-mails on your personal computer) to the non-IT employees. The directive to non-IT employees could be incorporated into a retention directive covering paper records.⁷⁶

ensure consistent compliance, to the extent reasonably possible, electronic evidence retention should be just that – done electronically – where human intervention will be only minimally needed. It is, of course, still advisable to notify employees of their personal retention obligations. See *infra* § IV(F).

⁷³ See, e.g., *Danis v. USN Communications, Inc.*, No. 98 C 7482, 2000 U.S. Dist. LEXIS 16900 (N.D. Ill. Oct. 23, 2000); *In re Prudential Ins. Co. of Am. Sales Practices Litig.*, 169 F.R.D. 598, 612-15 (D.N.J. 1997); *Nat’l Ass’n of Radiation Survivors v. Turnage*, 115 F.R.D. 543, 553 (N.D. Cal. 1987).

⁷⁴ *In re Prudential*, 169 F.R.D. at 615 (after court enters retention order, senior management must “initiate a comprehensive document preservation plan and distribute it to all employees”).

⁷⁵ *Id.* at 613 (concluding that e-mail distribution of preservation directive was inadequate because some witnesses testified that they ignored e-mails and other witnesses lacked access to e-mail).

⁷⁶ See Appendix A, Exemplar Preservation Directive to Non-IT Personnel.

When preparing the retention directive, the admonition to preserve and not destroy documents should be set forth in a special font or style. The directive should describe the nature of the pending litigation, the company's discovery obligations, and the ramifications for failing to comply.⁷⁷ It may be useful to include a list of sample electronic evidence that should be retained and urge employees to err on the side of saving too much electronic evidence rather than too little. The directive should be issued promptly because, as discussed below, destruction of electronic evidence may be sanctionable. A party can use whatever means are necessary to convey the information to its employees, but some courts have determined that all employees handling information that may be discoverable, not just management, need to be apprised of the litigation and the party's discovery obligations.⁷⁸ A party should communicate the preservation obligation to all relevant persons, including outside vendors, contractors, and other third parties. "Depending on the scope and duration of the litigation, it may be advisable to repeat the notice periodically in at least one form or location."⁷⁹

Finally, there should be some means for an employee to report noncompliance to senior management, and such reporting should be encouraged.⁸⁰ This could be accomplished, for instance, through a telephone hotline.⁸¹ The process should be anonymous in order to prevent retaliation and to encourage employees to cooperate with the litigation process. Employees also should be given a contact person for electronic evidence preservation questions.⁸² All complaints and allegations of noncompliance should be investigated.⁸³ If there is a

breach of compliance with the court's order, the court and opposing counsel should promptly be made aware of the noncompliance.⁸⁴ Delay can be seen as inexcusable.

G. Document Your Actions

Few cases, especially in the area of electronic evidence, offer detailed descriptions of searches found to be adequate or inadequate. The most useful lesson the cases teach is that litigants should be prepared to explain in detail what efforts they took to comply with their discovery obligations. Litigants should be able to explain where they looked, why they looked there, whom they asked, and what procedures they put in place to ensure complete and accurate compliance.⁸⁵ Therefore, the litigation triage team should carefully document its activities and be prepared to explain to the court the nature of its investigation and the steps taken to preserve electronic evidence.

H. Consider Counter-Attack

Parties with minimal electronic evidence face little risk in pushing the envelope of electronic discovery. It is a fact of litigation life that electronic

⁸⁴ See *In re Prudential*, 169 F.R.D. at 612 (court and counsel should be notified promptly of destruction); *Keir*, 2003 WL 21997747, at *13 (party that destroyed electronic evidence it was ordered to keep "could have promptly investigated what had gone wrong and reported the results of its investigation in a forthcoming manner to the plaintiffs and the Court"); *Nat'l Ass'n of Radiation Survivors*, 115 F.R.D. at 553 (finding bad faith violation of retention order for failing to disclose noncompliance with court order, hiding noncompliance with court order, and threatening retaliation against employees who disclosed the destruction).

⁸⁵ See, e.g., *Wiginton*, 2003 WL 22439865, at *5, 6 (holding that defendant should have preserved all relevant documents for key individuals and rejecting defendant's argument that preserving relevant data was cost prohibitive when there was no description about attempts to filter e-mails or search by key words); *Gratton v. Great Am. Communications*, 178 F.3d 1373, 1375 (11th Cir. 1999) (per curiam) (affirming district court's dismissal order; among other discovery violations, plaintiff failed to provide a detailed search description as required by court order); *Nat'l Ass'n of Radiation Survivors*, 115 F.R.D. at 552 (chastising in-house counsel who had no recollection of giving staff any instructions and for simply sending discovery requests to various department heads, leaving them to interpret the requests and to provide responsive material); *Bratka v. Anheuser-Busch Co.*, 164 F.R.D. 448, 461 (S.D. Ohio 1995) (characterizing in-house counsel's efforts as "grossly negligent"; in-house counsel assigned discovery requests to a layman without supervision or instructions); compare *Comeau v. Rupp*, 810 F. Supp. 1127, 1165-66 (D. Kan. 1992) (declining sanctions where the FDIC gave detailed explanations of its search).

⁷⁷ *In re Prudential*, 169 F.R.D. at 612 n.8, 615.

⁷⁸ *Danis*, 2000 U.S. Dist. LEXIS 16900, at *42 (criticizing company's approach of communicating only with managers and not ensuring that communication reached all necessary employees); but see *Sedona Principles* at 22 ("The notice does not need to reach all employees, only those reasonably likely to maintain documents relevant to the litigation or investigation.").

⁷⁹ *Sedona Principles* at 22.

⁸⁰ *In re Prudential*, 169 F.R.D. at 612 (company should encourage and facilitate reporting).

⁸¹ *Id.* at 617 (ordering company to establish telephone hotline to facilitate reports of document destruction).

⁸² *Id.* at 612 (noting in findings of fact that company had not designated specific individual "as the primary contact source for information about document preservation").

⁸³ See *Nat'l Ass'n of Radiation Survivors*, 115 F.R.D. at 553-54 (referring to failure to investigate reports of noncompliance).

discovery is expensive, time-consuming, and fraught with traps, even for sophisticated litigants. As a result, discovery of electronic evidence has been and will continue to be used tactically by parties who have little risk if the same kind of discovery is pursued against them. On the other hand, as between two parties with roughly equal collections of relevant electronic evidence, firing the first shot of electronic discovery requests could result in mutually assured self-destruction. Nevertheless, discovery of electronic evidence is going to happen. In litigation between larger enterprises, a litigant that receives extensive electronic discovery requests likely has a valid reason and should consider serving similar discovery on the other party. At the very least, it might provide a basis for negotiating a reasonable scope of electronic discovery for both sides. Further, large litigants should not automatically shy away from initiating electronic discovery against individual plaintiffs. There are cases, especially in lawsuits involving claims of discrimination or theft of company information, where individual parties were caught destroying potentially relevant electronic evidence.⁸⁶

I. Audit Compliance With The Preservation Plan

Parties who have implemented electronic evidence preservation steps may want to consider auditing compliance with their preservation program. Litigation consultants and counsel can design statistically sound audit plans to help a litigant determine whether it is meeting its preservation obligations. A recent case, *Landmark Legal Foundation v. EPA*,⁸⁷ highlighted the need to ensure that preservation obligations are fulfilled. In that case, the EPA's normal document retention policy resulted in the destruction of e-mails that were covered by a preservation order.⁸⁸ Even though the EPA's office of general counsel had notified employees of the need to preserve evidence, the court found that EPA had not

⁸⁶ See, e.g., *Anderson v. Crossroads Capital Partners, LLC*, No. Civ. 01-2000 ADM/SRN, 2004 WL 256512, *8 (D. Minn. Feb. 10, 2004) (holding that jury would be given adverse inference instruction where alleged sexual harassment plaintiff destroyed electronic evidence on hard drive); *Miller v. Time-Warner Communications, Inc.*, No. 97 Civ. 7286(JSM), 1999 WL 739528, at *1 (S.D.N.Y. Sept. 22, 1999) (dismissing plaintiff's discrimination complaint where plaintiff's deliberate attempt to destroy evidence was exacerbated by her repeated perjury on subject); *Playboy Enters., Inc. v. Welles*, 60 F. Supp. 2d 1050 (S.D. Cal. 1999) (allowing discovery of deleted e-mails on defendant's personal computer).

⁸⁷ 272 F. Supp. 2d 70 (D.D.C. 2003).

⁸⁸ *Id.* at 78.

taken steps to modify its procedures.⁸⁹ The EPA was held in contempt and required to pay legal fees.⁹⁰

J. Continually Evaluate The Preservation Plan

The triage team needs to be diligent in monitoring and, if necessary, modifying the preservation plan. The allegations and arguments in the case will certainly evolve over time, as will the team's level of knowledge of the company's computer systems. The preservation plan needs to adapt to those changes.

V. WHAT COULD HAPPEN TO PARTIES WHO FAIL TO PRESERVE

Since Texas does not recognize spoliation as a stand-alone tort,⁹¹ there are two legal principles available in civil litigation in Texas to punish parties who do not preserve evidence: an adverse inference jury instruction and civil sanctions.⁹²

A. Adverse Interference Jury Instruction

As described by one court, the sanction of an adverse inference jury instruction serves two functions: "The first is remedial: where evidence is destroyed, the court should restore the prejudiced party to the same position with respect to its ability to prove its case that it would have held if there had been no spoliation."⁹³ The second rationale is punitive: "allowing the trier of fact to draw the inference presumably deters parties from destroying relevant evidence before it can be introduced at trial."⁹⁴ An adverse inference jury instruction is used when the court finds a deliberate destruction of relevant evidence or when a party fails to produce relevant evidence or to explain its non-production.⁹⁵ Courts are divided on the

⁸⁹ *Id.* at 78-79.

⁹⁰ *Id.* at 89.

⁹¹ *Trevino*, 969 S.W.2d at 952.

⁹² *Id.* at 954 (Baker, J., concurring) ("When a party believes that another party has improperly destroyed evidence, it may either move for sanctions or request a spoliation presumption instruction.").

⁹³ *Turner v. Hudson Transit Lines, Inc.*, 142 F.R.D. 68, 74 (S.D.N.Y. 1991).

⁹⁴ *Id.* (quoting *Nation-Wide Check Corp. v. Forest Hills Dist., Inc.*, 692 F.2d 214, 218 (1st Cir. 1982)).

⁹⁵ *Wal-Mart*, 106 S.W.3d at 721; see *King v. Ill. Cent. R.R.*, 337 F.3d 550, 556 (5th Cir. 2003) ("An adverse inference based on the destruction of potential evidence is predicated on the 'bad conduct' of the defendant.") (citing *United States v. Wise*, 221 F.3d 140, 156 (5th Cir. 2000)); *Anderson*, 2004 WL 256512, at *8 (holding that jury would be given adverse inference jury instruction when alleged

level of culpability necessary to support an adverse inference sanction. Some courts have held that an adverse inference is not available without a showing that the destruction of evidence was intentional.⁹⁶ Others have held that negligent or reckless destruction of evidence may support an adverse inference.⁹⁷

“Depending on the severity of prejudice resulting from the particular evidence destroyed, the trial court can submit one of two types of [spoliation] presumptions.”⁹⁸ The more severe instruction is a rebuttable presumption, which is used when the nonspoliator cannot make a prima facie case without the destroyed evidence.⁹⁹ The jury is instructed to presume that the destroyed evidence was unfavorable to the spoliator unless the spoliator can disprove the presumed fact.¹⁰⁰ The second, less severe, type of presumption is “merely an adverse presumption that the evidence would have been unfavorable to the spoliating party,” but “it does not relieve the nonspoliating party of the burden to prove each element of its case.”¹⁰¹

B. Civil Sanctions

1. Federal Sanctions Rules

The court’s authority to impose sanctions for destruction of evidence arises both under Rule 37 and under the court’s inherent powers.¹⁰² Thus, although

sexual harassment plaintiff “intentionally destroyed evidence and thus attempted to suppress the truth”).

⁹⁶ See, e.g., *Britt v. Block*, 636 F. Supp. 596, 606-07 (D. Vt. 1986) (negligent destruction of records not sufficient to give adverse inference); *INA Aviation Corp. v. United States*, 468 F. Supp. 695, 700 (E.D.N.Y. 1979) (“[O]ne cannot justify the drawing of [an adverse] inference when the destruction of evidence is unintentional or where the failure to produce evidence is satisfactorily explained.”).

⁹⁷ See, e.g., *Pressey v. Patterson*, 898 F.2d 1018, 1024 (5th Cir. 1990); *Turner*, 142 F.R.D. at 75 (“[T]his sanction should be available even for the negligent destruction of documents if that is necessary to further the remedial purpose of the inference.”); *Trevino*, 969 S.W.2d at 957 (Baker, J., concurring) (“Because parties have a duty to reasonably preserve evidence, it is only logical that they should be held accountable for either negligent or intentional spoliation.”).

⁹⁸ *Trevino*, 969 S.W.2d at 960 (Baker, J., concurring).

⁹⁹ *Id.* (Baker, J., concurring).

¹⁰⁰ *Id.* (Baker, J., concurring).

¹⁰¹ *Id.* at 960-61 (Baker, J., concurring).

¹⁰² See *Silvestri*, 271 F.3d at 590; *Reilly v. NatWest Mkts. Group, Inc.*, 181 F.3d 253, 267 (2d Cir. 1999); *Wiginton*, 2003 WL 22439865, at *3 n.5; *Turner*, 142 F.R.D.

Rule 37 sanctions are only available if a party has failed to comply with a court order, a court can exercise its inherent powers to impose sanctions for spoliation even without violation of a court order.¹⁰³ “Rule 37(b)(2) provides a non-exhaustive list of possible sanctions, which include ordering that certain facts be taken as established at trial; that the disobedient party may not oppose adverse claims or support its own defense at trial; that pleadings may be stricken, the action dismissed, or a default judgment issued against the disobedient party; and that an order treating the failure to obey the prior order as a contempt of court may be issued.”¹⁰⁴

In addition, the court may require the non-complying party to pay all reasonable expenses, including attorney’s fees, incurred by the moving party as a result of the failure to comply.¹⁰⁵ The court must award these expenses unless it finds that the party’s failure to comply was “substantially justified,” or that, under the circumstances, an award of expenses would be “unjust.”¹⁰⁶ The amount of monetary damages awarded must, however, be related to the expenses incurred as a result of the discovery violations; otherwise, the monetary damages are not compensatory, but are punitive and thus can be awarded only pursuant to the court’s criminal contempt

at 72. See also *Pressey*, 898 F.2d at 1021 (trial judge given broad discretion to craft remedies under Rule 37(b)).

¹⁰³ See *Turner*, 142 F.R.D. at 72 (citing *In re Air Crash Disaster near Chicago, Illinois on May 25, 1979*, 90 F.R.D. 613, 620-21 (N.D. Ill. 1981)); see also *West v. Goodyear Tire & Rubber Co.*, 167 F.3d 776, 779 (2d Cir. 1999) (“Even without a discovery order, a district court may impose sanctions for spoliation, exercising its inherent power to control litigation.”); cf. *Pressey*, 898 F.2d at 1021 (a trial court’s discretion to impose sanctions under its inherent power is limited to instances of bad faith or willful abuse of the judicial process).

¹⁰⁴ *Thompson*, 219 F.R.D. at 102; see Fed. R. Civ. P. 37(b)(2); *Landmark*, 272 F. Supp. 2d at 77-79 (finding contempt of court for reformatting hard drives and erasing back-up tapes after counsel had received notice of preservation order but had failed to communicate with client).

¹⁰⁵ See *Ill. Tool Works, Inc. v. Metro Mark Prods. Ltd.*, 43 F. Supp. 2d 951, 954-56, 960-61 (N.D. Ill. 1999) (ordering attorneys’ fees and costs where court found that defendants purposely tried to prevent plaintiff from obtaining information from computer, defendants’ lawyers offered no information about what they did to explain the court’s computer ruling to their clients, and there was evidence that records custodian had deliberately tried to damage the computer).

¹⁰⁶ See Fed. R. Civ. P. 37(a)(4)(B); *Perkins v. Gregg County, Texas*, No. 6:94-CV-328, 1996 WL 61769, at *3 (E.D. Tex. Feb. 5, 1996).

powers.¹⁰⁷ Expenses may be awarded against the uncooperative party or its attorney or both.¹⁰⁸

The courts have made clear that failure to preserve evidence can result in the harshest of sanctions – dismissal.¹⁰⁹ The dismissal sanction “should only be employed ‘in extreme situations where there is evidence of willfulness, bad faith or fault by the non-complying party.’”¹¹⁰ While dismissal is an extreme sanction, “a court is not required to first impose less drastic sanctions.”¹¹¹

2. Texas Sanctions Rules

Texas state courts can impose sanctions under Texas Rule 215(3) or under the courts’ inherent power, which applies in circumstances where Rule 215(3) might not apply, such as pre-litigation destruction of

evidence.¹¹² Courts have broad discretion to fashion appropriate remedies on a case-by-case basis “to restore the parties to a rough approximation of their positions if all evidence were available.”¹¹³ Courts should weigh the degree of the spoliator’s culpability and the prejudice to the other side in fashioning a remedy.¹¹⁴ In Texas, the penalties for failure to preserve relevant evidence are similar to those available under the federal rules, such as dismissal or default judgment if the conduct is egregious and prejudice to the other party is great.¹¹⁵ To determine if sanctions or a spoliation presumption are justified, a court must determine: “(1) whether there was a duty to preserve evidence; (2) whether the alleged spoliator either negligently or intentionally spoliated evidence; and (3) whether the spoliation prejudiced the nonspoliator’s ability to present its case or defense.”¹¹⁶

VI. CONCLUSION

Identifying relevant electronic evidence and taking the proper steps to preserve it is as much an art as a science, where the best tool a litigant could have would be a crystal ball. Ignoring, misunderstanding, or trying hard but simply guessing wrong on the duty to preserve can, in some circumstances, be outcome-determinative. Experienced counsel and technically proficient computer experts can help litigants safely traverse the electronic evidence preservation minefield.

¹⁰⁷ See *Martin v. Brown*, 63 F.3d 1252, 1263-64 (3d Cir. 1995).

¹⁰⁸ See Fed. R. Civ. P. 37(a)(4)(A).

¹⁰⁹ See *Winters v. Textron, Inc.*, 187 F.R.D. 518, 519-20 (M.D. Pa. 1999) (noting that default judgments are drastic sanctions); see also *Lafarge Corp. v. M/V Macedonia Hellas*, No. 99-2648 § K(5), 2000 U.S. Dist. LEXIS 15963, at *16 (E.D. La. Oct. 23, 2000) (“Dismissal with prejudice for violation of a discovery order is appropriate if 1) the refusal to comply results for bad faith or willfulness and is accompanied by delay or contumacious conduct; 2) the violation of the discovery order is attributable to the client instead of the attorney; 3) the violating conduct substantially prejudices the other party; and 4) a less drastic sanction would not achieve the same result.”).

¹¹⁰ *Wiginton*, 2003 WL 22439865, at *6 (quoting *Danis v. USN Communications, Inc.*, No. 98 C 7482, 2000 WL 1694325, at *33 (N.D. Ill. Oct. 20, 2000)); see also *Pressey*, 898 F.2d at 1021 (a finding of bad faith or willful misconduct is usually required to strike pleading or dismiss case under Rule 37); *Procter & Gamble Co. v. Haugen*, No. 1:95CV94 DAK, 2003 WL 22080734 (D. Utah Aug. 19, 2003) (dismissing case with prejudice in part for failure to preserve relevant electronic data known to be critical to case).

¹¹¹ *Kucala Enters.*, 2003 WL 21230605, at *4 (dismissing suit and imposing costs where plaintiff used computer program to eliminate potential electronic evidence); *Danis*, 2000 U.S. Dist. LEXIS 16900, at *94-95 (a court “is not always required ‘to fire a warning shot’ before imposing a stiff sanction”). But see *Pressey*, 898 F.2d at 1021 (courts should consider whether less drastic remedy tailored to meet the misconduct would better serve the purposes of Rule 37 rather than a case-dispositive sanction); *Tandycrafts, Inc. v. Bublitz*, No. 3:97-CV-1074-T, 2002 U.S. Dist. LEXIS 3353, at *10 (N.D. Tex. Feb. 28, 2002) (finding that sanction of summary judgment for spoliation of evidence was too harsh and should not have been imposed when a lesser remedy was available).

¹¹² *Trevino*, 969 S.W.2d at 958-59 (Baker, J., concurring) (“Trial courts have broad power to police litigants and protect against evidence spoliation.”).

¹¹³ *Wal-Mart*, 106 S.W.3d at 721.

¹¹⁴ *Trevino*, 969 S.W.2d at 959 (Baker, J., concurring).

¹¹⁵ *In re Dynamic Health, Inc.*, 32 S.W.3d 876, 885 (Tex. App. – Texarkana 2000, pet. denied) (upholding order of “death penalty sanctions” in face of egregious conduct by spoliator, great prejudice to the non-spoliating party, and lack of effective lesser sanction to cure prejudice).

¹¹⁶ *Trevino*, 969 S.W.2d at 954-55 (Baker, J., concurring).

APPENDICES

APPENDIX A

SAMPLE PRESERVATION DIRECTIVE

**PRIVILEGED AND CONFIDENTIAL
ATTORNEY-CLIENT COMMUNICATION**

TO: [Insert list of recipients]
FROM: Legal Department
RE: Records Retention Directive - [Insert name of lawsuit]
DATE: [Insert date]

PRESERVE DOCUMENTS AND ELECTRONIC INFORMATION

DO NOT DESTROY

[Company] has been sued in [state] by [specify or generic name of plaintiff] claiming [describe causes of action, e.g., “breach of contract, fraud, tortious interference” and general description of factual issues, e.g., “arising out of company’s acquisition of Acme Corp.”]. The court overseeing this case has entered an order requiring [Company] to retain and preserve certain types of records and electronic information. A copy of the order is attached.

**IT IS IMPORTANT FOR YOU TO CAREFULLY READ THIS MEMORANDUM AND THE
ATTACHED COURT ORDER.**

This Memorandum restates and supplements the information contained in the Legal Department’s previous memoranda of [dates]. This confirms that until further notice, the following categories of records (regardless of date or retention policy) SHALL be retained, to the extent they are available, in all forms, including hard copy, electronic, and audio/video/broadcast:

- 1.
 - 2.
 - 3.
 - 4.
-

If you have any doubts as to whether a record would be included in the scope of this Memorandum, retain it.

We understand that this is a burden to your operations. However, it is absolutely critical that these records continue to be retained.

To ensure that all responsive documents are identified and retained, please use the following checklist as a guide when searching for responsive materials:

- | | |
|---|---|
| <input type="checkbox"/> Desktop / Desk drawers | <input type="checkbox"/> Briefcase |
| <input type="checkbox"/> File Cabinets | <input type="checkbox"/> Home Files |
| <input type="checkbox"/> Electronic Mail | <input type="checkbox"/> Notebooks / Calendar (Appointment Book) |
| <input type="checkbox"/> Personal Digital Assistants (“PDA”) (e.g., Palm, BlackBerry) | <input type="checkbox"/> “Personal” and “Confidential” Files |
| <input type="checkbox"/> Computer Hard Drive (desktop and/or laptop) | <input type="checkbox"/> Voicemail, Tape Recordings |
| <input type="checkbox"/> Computer Diskettes, CDs, or other Media | <input type="checkbox"/> Onsite and Offsite Storage Areas |
| <input type="checkbox"/> Support Staff Files | <input type="checkbox"/> Microfilm / Microfiche |
| <input type="checkbox"/> Central / Group Files | <input type="checkbox"/> Other Location that You Believe May Contain Responsive Information (e.g., materials held by prior persons in the position) |
| <input type="checkbox"/> Reading Files | |

SERIOUS SANCTIONS POSSIBLE. Failure to adhere to these requirements could result in serious legal consequences for the Company and/or its employees, including potential civil and criminal sanctions or contempt for non-compliance.

READ ATTACHED COURT ORDER. A copy of the court order requiring retention of these materials is attached. Read it.

POST NOTICE AND INFORM EMPLOYEES. You must insure that those with record retention responsibilities in your department are notified of this directive. This retention notice must be posted in an area where all employees who have access, possession, custody, or control of the materials to be retained can see it.

IMMEDIATELY REPORT NON-COMPLIANCE. If you become aware of any failure to adhere to these retention requirements, you should report it immediately to [name] in the Legal Department at [phone]. If you wish to make an anonymous report regarding the failure to adhere to these retention requirements, you should report it immediately to _____.

SERIOUS EMPLOYMENT CONSEQUENCES POSSIBLE. Failure to adhere to these requirements could result in serious employment consequences, up to and including termination.

ASK QUESTIONS. Should you have any questions regarding this directive, please contact [name] in the Legal Department at [phone]. Thank you for your cooperation on this important matter.

APPENDIX B

QUESTIONS FOR CLIENT REGARDING ELECTRONIC EVIDENCE

A. System Profile

1. Obtain a copy of the organizational chart for the IT department.
2. Who is responsible for operating, maintaining, and administering the system? Any third-party vendors?
3. What are the characteristics of the computer system presently in place? What were the characteristics of the computer system at the time relevant to the threatened or pending litigation?
4. What number and types of desktop and laptop computers are used?
5. What types of operating systems are used?
6. What are your network architecture and usage policies?
7. What network software is used?
8. What network server hardware is used? (Mainframes, mini computers, e-mail servers, file servers, fax servers, voice-mail servers?)
9. What are the file-naming and location-saving conventions?
10. How are shared files structured and named on the system?
11. What specific software is used (including software applications for things such as calendars, project management, accounting, word processing, and database management)?

B. Data Retention and Destruction Protocols

1. Is there a written policy for the retention and destruction of electronic information? What are the policies and procedures (now and during relevant time frame) for document, computer, electronic data, and electronic media retention, preservation, and destruction? Obtain copy of written policies.
2. How are corporate records retention policies and schedules applied to backed up and/or archived electronic data?
3. Do you have a file purge schedule?

C. Back-ups

1. Obtain copy of back-up schedule.
2. Who is responsible for archiving or backing up the system? Any third-party vendors?
3. Who has access to back-ups? Who actually performs the back-ups?
4. What is the back-up media used (tapes, discs, drives, cartridges)?
5. Does the IT department conduct daily, weekly, monthly, or other regular back-ups of the systems?

6. Is the back-up process automated?
7. Does the IT department keep back-up tapes before recycling or destroying them? What is the tape rotation cycle? Have any tapes been pulled from the rotation? Are any back-up tapes (e.g., the last day of the month), pulled from the normal rotation and stored for a longer period of time?
8. What is the location of the back-up media (off-site storage, out-of-state storage, etc.)? How does the media get to the storage location? How are tapes stored?
9. What is the indexing and control system for back-up tapes?
10. Describe all non-routine back-up tapes or other media for each computer, network, electronic media, and electronic data (e.g., back-ups made for system upgrades, file migration or consolidation, computer upgrades, special projects, software application upgrades, hardware replacement, off-site storage redundant systems, test environments, disaster recovery, and Y2K).
11. Have you ever restored data from a back-up tape? When? What data was restored? Why was the data restored? Was the restoration successful? What were the resources required to perform the restoration?

D. Security

1. What security software/utilities are used?
2. Are passwords or encrypted files used on any of the computer systems? Describe what is protected. How are the files protected? Who has super-user status?
3. How do those outside of the company access the computers?

E. Former Employees

1. What happens to the hard drive of an employee who leaves the company?
2. Does the department create a “mirror image” of the employee’s data in the event that the data may have future use, or does it wipe the hard drive clean for use by another employee?
3. Are files routinely deleted from servers when employees leave or are reassigned?
4. Are e-mail/user server accounts closed/purged when an employee leaves?
5. Are passwords and access codes revoked/changed when an employee leaves?

F. Internet

1. Does the company provide internet access for its employees? What employees have access?
2. What internet service provider (ISP) was used and what was the method used to connect to the internet?
3. What internet browsers are used?
4. Do any employees subscribe to or participate in internet newsgroups or chat groups in the course of their employment? Who are the users, and what are the services that they subscribe to or participate in?

5. Are there manuals, policies, or guidelines for employee access and use of internet resources? Any restrictions on, controls over, or monitoring of employee use of internet resources?

G. E-mail

1. Who is responsible for administering the e-mail system?
2. What type of e-mail system is used, including software, number of users, location of mail files, and password usage?
3. Does the company's e-mail system have an auto delete feature, or does the owner of the individual e-mail account have to "empty" the deleted folder associated with the mailbox? Even when users delete messages from their machines, does the e-mail server store copies elsewhere?
4. Are "janitorial" programs run to purge e-mail?
5. Can users access their e-mail remotely?
6. How many specific e-mail back-up tapes are presently in storage from past usage?
7. What is the frequency with which back-up tapes have been used to reconstruct or search for missing e-mails?

H. Databases, Files, and Tables

1. Who is responsible for database design and maintenance, report design, database back-up, and user requests?
2. What types of databases are used? What type of database software is used?
3. What are the fields of information in the databases?
4. Who enters information into the database? What is the source of information?
5. How is the database accessed? Who are the users? What are the access security levels for users?
6. Are queries stored? If so, where?
7. What are the outputs/responses to queries? Are the responses stored? If so, where?
8. Are any standard reports prepared on a routine basis? Who are the recipients? Are the reports stored? If so, where?

I. Telephone & Voice Mail

1. What telephone equipment is provided to employees (including desktop telephones, cell phones, pagers, laptop modems, calling cards, telephony software, and contact management software)?
2. Does the company keep phone records, logs of incoming and outgoing calls, invoices, and contact management records?
3. Is there a voice mail retention policy in place? Is there an automatic system? Can users store voice mail messages, at their option? If so, in what format?

J. Other

1. What portable devices (not connected to the network) are used by employees in the course of their employment (including digital recorders, digital cameras, and external storage devices)?
2. Do employees use PDAs?
3. Do employees have home computers used for business purposes?
4. Do you keep or discard outdated back-up drives or software?
5. What is the process followed when disposing of or recycling desktop and/or notebook computers?
6. What are the disk or tape labeling conventions?
7. Do employees have access cards that permit entry into the parking garage or specific areas in the building?
8. Does the company have video surveillance records?