

**PRESERVATION:
COMPETENTLY NAVIGATING BETWEEN ALL AND NOTHING**

Lauren Wheeling Waller *

Cite as: Lauren Wheeling Waller, *Preservation: Competently Navigating Between All and Nothing*, 22 RICH. J.L. & TECH. 7 (2016), <http://jolt.richmond.edu/v22i3/article7.pdf>.

I. INTRODUCTION

[1] Merriam-Webster defines “competent” as “having requisite or adequate ability or qualities.”¹ All professions require competence to be successful—from chefs, to tailors, to NFL quarterbacks. Without the adequate ability to poach an egg, alter suits, or read defenses, they lose patrons, customers, or—in the case of a quarterback—games and fans. Lawyers are no different. Without competence, they may not be successful. However, lawyers are different than the NFL quarterback in that they have an explicit duty of competence to their clients. The Model Rules of Professional Conduct provide “[a] lawyer shall provide competent representation to a client. Competent representation requires the legal knowledge, skill, thoroughness, and preparation reasonably

* Lauren Wheeling Waller is a partner at Williams Mullen and chairs the firm’s e-Discovery and Information Governance Practice Group. She is an experienced litigator and provides guidance in crafting defensible and uniform approaches to records management and retention, litigation hold implementation, as well as managing complex e-Discovery projects in commercial litigation and investigations. She has written and spoken frequently on electronic discovery topics and is a member Working Group I on Electronic Document Retention and Production of The Sedona Conference.

¹ *Competent*, MERRIAM-WEBSTER, <http://www.merriam-webster.com/dictionary/competent>, archived at <https://perma.cc/VZ57-Z6TR> (last visited Feb. 25, 2016).

necessary for the representation.”² The comments to the Model Rules make it clear that competency also requires that lawyers “keep abreast of changes in the law and its practice, *including the benefits and risks associated with relevant technology . . .*”³ With this sentence, attorneys can no longer simply put up their hands and say, “it’s e-mail and text messages, I don’t know how nor do I want to handle that.”

[2] Additionally, some State Bars implementing their own Rules of Professional Conduct have decided that attorney competence applies to handling electronically stored information (“ESI”), and at a minimum, that attorneys be able to carry out the following:

- [I]nitially assess e-[D]iscovery needs and issues, if any;
- [I]mplement/cause to implement appropriate ESI preservation procedures;
- [A]nalyze and understand a client’s ESI systems and storage;
- [A]dvice the client on available options for collection and preservation of ESI;
- [I]dentify custodians of potentially relevant ESI;
- [E]ngage in competent and meaningful meet and confer with opposing counsel concerning an e-[D]iscovery plan;
- [P]erform data searches;
- [C]ollect responsive ESI in a manner that preserves the integrity of that ESI; and
- [P]roduce responsive non-privileged ESI in a recognized and appropriate manner.⁴

² MODEL RULES OF PROF’L CONDUCT R. 1.1 (2014).

³ MODEL RULES OF PROF’L CONDUCT R. 1.1 cmt. 8 (2014) (emphasis added).

⁴ State Bar of Cal. Standing Comm. on Prof’l Responsibility & Conduct, Formal Op. 2015-193, 3–4 (2015) [hereinafter Cal. Ethics Op.] (emphasis added) (internal citations omitted).

[3] Attorneys now need to have an understanding of the components of the Electronic Discovery Reference Model⁵ and the tools available to assist in each part of that process. If they do not have the requisite understanding, they need to associate with someone who does.⁶

[4] Preservation of ESI is implicated in at least five of the competencies specifically listed in a California Rules of Professional Conduct's Formal Opinion,⁷ but preservation for some lawyers can be a scary concept. Why? For one, data never sleeps.⁸ Every minute of the day, people generate data in the form of e-mails, Instagrams, Tweets, and Snapchats.⁹ If you compare the data generated in 2012 to that created in 2015, not only has the amount of data increased, but also the type of data created has increased with the proliferation of new applications that create

⁵ See *EDRM Stages*, EDRM, <http://www.edrm.net/resources/edrm-stages-explained>, archived at <https://perma.cc/D63L-HC9E> (last visited Feb. 25, 2016).

⁶ See Cal. Ethics Op., *supra* note 4, at 3; see also *HM Electronics, Inc. v. RF Techs., Inc.*, No. 12cv2884-BAS-MDD, 2015 WL 4714908, at *24 (S.D. Cal. Aug. 7, 2015) (holding that an “attorney’s duty to supervise the work of consultants, vendors, and subordinate attorneys is non-delegable. ‘An attorney must maintain overall responsibility for the work . . . ,’ and, must do so by *remaining regularly engaged* in the . . . work.”) (internal citations omitted) (emphasis in original).

⁷ See Cal. Ethics Op., *supra* note 4, at 3–4. (“[I]nitially assess e-[D]iscovery needs and issues, if any; [I]mplement/cause to implement appropriate ESI preservation procedures; [A]nalyze and understand a client’s ESI systems and storage; [A]dvice the client on available options for collection and preservation of ESI; [I]dentify custodians of potentially relevant ESI; [C]ollect responsive ESI in a manner that preserves the integrity of ESI”).

⁸ See generally *Data Never Sleeps 3.0*, DOMO, https://web-assets.domo.com/blog/wp-content/uploads/2015/08/15_domo_data-never-sleeps-3_final1.png, archived at <https://perma.cc/HN24-72YD> (last visited Feb. 11, 2016).

⁹ See *id.*

data.¹⁰ Identifying the type of data that needs to be preserved and how it needs to be preserved can be complicated because of this ever-changing data landscape.

[5] Additionally, preservation provokes fear in the heart of many attorneys, because failing to preserve potentially relevant evidence can have significant adverse consequences for not only the client in the lawsuit but also for the attorneys involved.¹¹ Attorneys, however, now have more guidance regarding the imposition of sanctions in Federal Court, as the Federal Rules of Civil Procedure were amended to clarify when a court can impose sanctions for the failure to appropriately preserve evidence, including when evidence is intentionally destroyed.¹²

[6] Even with the amendments to the Rules, the following questions still exist for every piece of litigation:

- When does the duty to preserve arise?

¹⁰ Compare *id.*, with *Data Never Sleeps 2.0*, DOMO, www.domo.com/learn/data-never-sleeps-2, archived at <https://perma.cc/83QJ-HM8Q> (last visited Feb. 11, 2016), and *Data Never Sleeps*, DOMO, www.domo.com/blog/2012/06/how-much-data-is-created-every-minute, archived at <https://perma.cc/Q5LW-ZK4B> (last visited Feb. 11, 2016) (noting that applications such as Snapchat and Tinder were not identified in 2012 but generated vast amounts of data in 2015).

¹¹ See *Victor Stanley, Inc. v. Creative Pipe, Inc.*, 269 F.R.D. 497, 538–41 (D. Md. 2010) (recommending sanctions including permanent injunction and attorneys' fees); *Malibu Media, LLC v. Tashiro*, No. 1:13-cv-00205-WTL-MJD, 2015 U.S. Dist. LEXIS 64281, at *104 (S.D. Ind. May 18, 2015) (granting motion for sanctions for default judgment); *HM Elecs., Inc. v. RF Techs., Inc.*, No. 12cv2884-BAS-MDD, 2015 WL 4714908, at *31–35 (S.D. Cal. Aug. 7, 2015) (recommending adverse inference instruction, as well as other sanctions). As these cases indicate, EDRM preservation tends to be the area where attorneys and clients make the most mistakes.

¹² See FED. R. CIV. P. 37(e) (allowing for sanctions only when information is lost and cannot be replaced, and the court finds that another party is prejudiced from the loss or that the party acted with the intent to deprive the other party of information).

- What must be preserved for the potential or current litigation?
- What steps can I take to competently preserve potentially relevant information?

[7] Is the answer to the above questions that every piece of data in your client’s possession must be preserved? No. Is the answer to preserve only e-mails a specific custodian sends to counsel on his or her own accord, without any further discussion with counsel? No. While there is no “one size fits all” answer to preservation, this article intends to guide practitioners through the preservation rubric outlined in the cases of “e-Discovery Canon,”¹³ as well as recent case law and the 2015 amendments to the Federal Rules of Civil Procedure. This article also outlines questions practitioners should ask their clients and themselves in order to competently identify and preserve ESI.

II. THE DUTY TO PRESERVE

[8] The first question that a lawyer must answer is whether the duty to preserve has been triggered. Common law creates the duty to preserve evidence, and litigants owe this duty to the court, not just the opposing party.¹⁴ Some commentators argue that the duty to preserve may be the most important duty a litigant has, in that failing to meet this duty can deprive the court of the ability to properly assess the claims of the parties

¹³ See *Pension Comm. of Univ. of Montreal Pension Plan v. Banc of Am. Sec., LLC*, 685 F. Supp. 2d 456, 461 (S.D.N.Y. 2010) [hereinafter *Pension Comm.*], *abrogated by* *Chin v. Port Auth. of N.Y. & N.J.*, 685 F.3d 135, 143 (2d Cir. 2012); *Rimkus Consulting Grp. v. Cammarata*, 688 F. Supp. 2d 598, 607 (S.D. Tex. 2010); *Victor Stanley, Inc.*, 269 F.R.D. at 499–500; *Zubulake v. UBS Warburg LLC (Zubulake V)*, 229 F.R.D. 422, 424 (S.D.N.Y. 2004), *Zubulake v. UBS Warburg LLC (Zubulake IV)*, 220 F.R.D. 212, 214 (S.D.N.Y. 2003).

¹⁴ See *Victor Stanley, Inc.*, 269 F.R.D. at 525 (noting “the duty to preserve evidence relevant to litigation of a claim is a duty owed to the *court*.”) (emphasis in original).

before it.¹⁵ This duty “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 the anticipated litigation.”¹⁶ In the context of litigation for plaintiffs, the duty arises before the lawsuit is filed, and for defendants when the lawsuit is served, at the very latest.¹⁷

[9] To be clear, though, whether a party is filing or has filed a lawsuit is not the test—it is the reasonable anticipation of litigation, in whatever form that takes. Recently, in *Clear-View Technologies, Inc. v. Rasnick*, Magistrate Judge Paul S. Grewal (no stranger to preservation and e-Discovery issues¹⁸) found that a text message sent to a defendant over two years before suit was filed and eight months before any preservation notice was sent to the defendant triggered the duty to preserve.¹⁹ Magistrate Judge Grewal stated that Plaintiff’s then-CEO “made clear in text messages to [defendants] that he was prepared to sue them for trying to interfere with” a potential business investment.²⁰ In his opinion, Judge Grewal noted that while the then-CEO later sent text messages apologizing for his previous texts, at no time did he take back his threat of

¹⁵ See Monica McCarroll, *Discovery and the Duty of Competence*, 26 REGENT U. L. REV. 81, 91 (2013).

¹⁶ *Silvestri v. Gen. Motors Corp.*, 271 F.3d 583, 591 (4th Cir. 2001).

¹⁷ See *Pension Comm.*, 685 F. Supp. 2d at 466.

¹⁸ See generally *Apple Inc. v. Samsung Elecs. Co., Ltd.*, 881 F. Supp. 2d 1132, 1132 (N.D. Cal. 2012).

¹⁹ See *Clear-View Techs., Inc. v. Rasnick*, No. 5:13-cv-02744-BLF, 2015 U.S. Dist. LEXIS 63579, at *3. The text message stated, in part, “[D]on’t call my shareholders with your b.s. That is [tortious] economic interference. I will not accept this. . . . [K]eep it up and you’ll find [yourself] in court[.] Call Clyde again and I sue. Mark my words.” *Id.* at *3–4 (alteration in original).

²⁰ *Id.* at *3.

litigation.²¹ In the context of non-lawsuit triggers, courts have also found that a presentation regarding potential patent infringement claims,²² ultimatums made to a CEO to “comply with [an] injunction” or face a lawsuit,²³ and of course, requests in writing that an individual or entity preserve evidence that may be relevant to a dispute trigger the duty to preserve.²⁴

[10] Accordingly, practitioners should not depend on the arrival of a complaint to trigger a client’s duty to preserve. While service of pleadings certainly can and does trigger the duty to preserve, once apprised of a potential dispute, practitioners should ask their clients not only about the facts of the potential dispute, but also how they communicated with the individuals involved with the potentially adverse party—in-person, telephone, e-mail, text messages, and/or any other medium of communication. As a practical matter, these queries will be easier the more you know about your client’s business and data landscape.²⁵ While a slip-and-fall, a failure to make a specified delivery under the terms of a contract, or a malfunction of a piece of equipment causing injury will remain clear triggers for the duty to preserve, practitioners should not overlook the wide variety of ways individuals now communicate with one

²¹ *See id.* at *21.

²² *See* Apple Inc., 881 F. Supp. 2d at 1145 (noting that the presentation from Apple provided Samsung with “more than just a vague hint” that litigation “was at least foreseeable, if not ‘on the horizon.’”).

²³ *In re* Napster, Inc. Copyright Litig., 462 F. Supp. 2d 1060, 1069 (N.D. Cal. 2006).

²⁴ *See, e.g.,* Altercare, Inc. v. Clark, 9th Dist. No. 12CA010211, 2013-Ohio-2785, at ¶ 2.

²⁵ While discussed only in the context of preservation below, information about a client’s data landscape prior to litigation should be part of an overall information governance effort. *See Information Governance Reference Model (IGRM)*, EDRM, www.edrm.net/projects/igrm, archived at <https://perma.cc/6F5N-D633> (last visited Mar. 18, 2016) [hereinafter IGRM].

another when analyzing whether and when the duty to preserve was triggered.

III. THE SCOPE OF PRESERVATION

[11] The duty to preserve evidence includes “an obligation to identify, locate, and maintain[] information that is relevant to specific, predictable, and identifiable litigation.”²⁶ The duty pertains, however, *only to relevant documents*.²⁷ Relevant documents include:

[A]ny documents or tangible things . . . made by individuals “likely to have discoverable information that the disclosing party may use to support its claims or defenses.” The duty also includes documents prepared for those individuals to the extent those documents can be readily identified (*e.g.*, from the “to” field in e-mails). The duty also extends to information that is relevant to the claims or defenses of any party, or which is “relevant to the subject matter involved in the action.” Thus, the duty to preserve extends to those employees likely to have relevant information—the “key players” in the case.²⁸

²⁶ *Apple Inc.*, 881 F. Supp. 2d at 1137; THE SEDONA CONFERENCE, THE SEDONA CONFERENCE COMMENTARY ON LEGAL HOLDS: THE TRIGGER & THE PROCESS 1 (Conor R. Crowley et al. eds., 2007), <https://thesedonaconference.org/download-pub/77>, archived at <https://perma.cc/EP4B-2AAY> (download required).

²⁷ See *Pension Comm.*, 685 F. Supp. 2d 456, 466 (S.D.N.Y. 2010), *abrogated by* *Chin v. Port Auth. of N.Y. & N.J.*, 685 F.3d 135, 143 (2d Cir. 2012).

²⁸ *Zubulake IV*, 220 F.R.D. at 217–18. While this case was decided under the pre-2015 amendment scope of discovery, it remains a seminal case in defining the scope of the duty to preserve.

The cases are clear on one point: once the duty to preserve is triggered, not every piece of data belonging to an organization must be preserved, just as every piece of paper belonging to an organization is not required to be preserved.²⁹ The cases outlined below demonstrate as much.

[13] In *Blue Sky Travel & Tours, LLC v. Al Tayyar*, the Fourth Circuit vacated and remanded the district court’s decision to impose severe sanctions on the defendant for failing to preserve certain invoices requested by the plaintiff.³⁰ In this breach of contract action, the plaintiff’s damages included a claim for lost profits, and in an effort to prove those lost profit claims, the plaintiff requested that the defendant produce certain invoices.³¹ When the defendant did not provide the invoices, the plaintiff moved to compel their production.³² The court granted the motion, but the defendant still did not produce the invoices because the documents were not retained.³³ The plaintiff then moved for sanctions, and the magistrate recommended the court grant the motion and provide an adverse inference instruction.³⁴ The problem with this recommendation and ruling, though, was that the magistrate judge ruled that the defendant had a duty to hold “all” documents, stating:

[W]hen this litigation started, the defendants were required by law to preserve. Any document retention policy you had

²⁹ *See id.* at 217 (noting that the duty to preserve does not require litigants to preserve “every shred of paper, every e-mail or electronic document, and every backup tape[.]”).

³⁰ *See Blue Sky Travel & Tours, LLC v. Al Tayyar*, 606 Fed. Appx. 689, 690 (4th Cir. 2015).

³¹ *See id.* at 691.

³² *See id.*

³³ *See id.* at 692.

³⁴ *See id.* at 692–93.

had to be stopped. . . . [o]nce you are put on notice that there is litigation pending, or once litigation starts, you are required . . . to stop [your] normal document retention policies and to preserve [ALL] documents because you don't know what may or may not be relevant.³⁵

[14] The Fourth Circuit vacated and remanded the magistrate's decision because the lower court used the incorrect standard for the duty to preserve.³⁶ The Fourth Circuit noted that a party may be sanctioned for spoliation if the party "(1) had a duty to preserve material evidence, . . . (2) willfully engaged in conduct resulting in the loss or destruction of that evidence, [and] (3) at a time when the party knew, or should have known, that the evidence was or could be relevant to the litigation."³⁷ The Fourth Circuit reiterated that a party is *not required to preserve all of its documents*, only documents that the party knew or should have known were or could be relevant to the parties' dispute.³⁸

[15] In *Wandering Dago, Inc. v. N.Y. State Office of Gen. Servs.*, the court had to decide whether officials in one governmental agency and their attorney could be sanctioned for the destruction of e-mails, according to the terms of an e-mail retention policy, belonging to another governmental agency.³⁹ More to the point, the court had to determine whether a preservation obligation for one governmental agency involved in a specific litigation automatically applies to every other governmental

³⁵ *Blue Sky Travel & Tours, LLC*, 606 Fed. Appx. at 692.

³⁶ *See id.* at 690.

³⁷ *Id.* at 697–98.

³⁸ *See id.*

³⁹ *See* *Wandering Dago Inc. v. N.Y. State Office of Gen. Servs.*, No. 1:13-CV-1053 (MAD/RFT), 2015 U.S. Dist. LEXIS 69375, at *1 (N.D.N.Y. May 29, 2015).

agency not involved in the litigation.⁴⁰ The court said no, as the defendant agencies in the litigation had no control over the other governmental agencies' e-mails.⁴¹ Therefore, the defendant agencies had no obligation to preserve the other non-party agencies' e-mails.⁴² The court noted that to require a governmental agency in litigation to preserve and produce documents belonging to another governmental agency not a party to the litigation would "subject all [] agencies, the legislature, the judiciary, quasi-state agencies, and possibly public authorities to disclosure scrutiny, notwithstanding their relative remoteness to the case."⁴³ The court found that "state agencies for most purposes are separate and distinct organs and should not be viewed in the aggregate."⁴⁴ Moreover, the court noted that requiring each governmental agency "and thousands of officials to institute a litigation hold every time a party contemplates or even commences litigation against another agency would paralyze the State."⁴⁵

[16] In *AMC Technology, LLC v. Cisco Systems, Inc.*, Magistrate Judge Grewal distinguished between documents parties are obligated to preserve and those that they are *not* obligated to preserve and that can be destroyed as part of a routine retention policy.⁴⁶ Pursuant to Cisco's document retention policy, Cisco reformatted departed employees' laptops and

⁴⁰ *See id.* at *1–2.

⁴¹ *See id.* at *22 ("Defendants correctly assert that they have no control over [Defendants'] emails. . .").

⁴² *See id.*

⁴³ *Id.* at *23 (quoting *N.Y. v. Amtrak*, 233 F.R.D. 259, 266 (N.D.N.Y. 2006)).

⁴⁴ *Wandering Dago Inc.*, 2015 U.S. Dist. LEXIS 69375, at *24.

⁴⁵ *Id.* at *24–25.

⁴⁶ *See AMC Tech., LLC v. Cisco Sys. Inc.*, No. 11-cv-3403 P, 2013 U.S. Dist. LEXIS 101372, at *4 (N.D. Cal. July 15, 2013).

deleted e-mail archives thirty days after an employee's departure.⁴⁷ After one employee's departure, and the deletion of his data, AMC requested his custodial data.⁴⁸ When Cisco did not provide the data because it had been destroyed according to its retention policy, AMC moved for spoliation sanctions.⁴⁹

[17] Judge Grewal held that sanctions were not warranted because Cisco was under no obligation to preserve his data at the time it was destroyed.⁵⁰ Judge Grewal underscored that the "scope of this duty is confined to what is reasonably foreseeable to be relevant to this action. Requiring a litigant to preserve all documents, regardless of their relevance, would cripple parties who are often involved in litigation"⁵¹ In its analysis, the court also noted that the disposal of the employee's documents "appears to have been routine—Cisco followed established company procedure, which deletes company emails and information within thirty days."⁵²

[18] These cases provide a framework for identifying the scope of preservation. While each case turns on its own unique facts, these cases demonstrate that preserving everything is not the requirement of the duty to preserve, as such a requirement would create inefficiencies for business and government entities attempting to carry out their daily functions. Moreover, they show that only those documents that are reasonably foreseeable to be relevant to the action at the time the duty is triggered

⁴⁷ *See id.* at *4.

⁴⁸ *See id.* at *5–7.

⁴⁹ *See id.*

⁵⁰ *See id.* at *10.

⁵¹ *AMC Tech., LLC*, 2013 U.S. Dist. LEXIS 101372, at *9.

⁵² *Id.* at *11.

must be preserved. Obviously, what is relevant can change during the course of an investigation. As a result, practitioners should continue to monitor what has been preserved and the pertinent issues in the litigation to continue to observe their preservation obligations.

A. Identifying What Must Be Preserved

[19] So the next question is: how do you identify and preserve documents that are potentially relevant to the parties' dispute? Understanding who created and possesses potentially relevant ESI—and how that ESI is stored—is the first step to competently complying with the duty to preserve. Not taking these steps can lead to the destruction of potentially relevant information, and adverse consequences for that destruction. *Brown v. Tellerate Holdings Ltd.* outlines the failings of practitioners in executing their duty to identify and preserve potentially relevant ESI, and thus provides a good description of what practitioners need to do to competently comply with their preservation obligations.

[20] In *Brown v. Tellerate Holdings Ltd.*, the court found that Tellerate's counsel "failed to uncover even the most basic information about an electronically-stored database of information" and that "as a direct result of that failure, took no steps to preserve the integrity of the information in that database."⁵³ In this age discrimination case, the plaintiffs requested reports from both of their accounts in salesforce.com, a web-based application that allows businesses to track sales activities, as well as a number of other employees' reports.⁵⁴ While at Tellerate, the plaintiff employees knew that Tellerate acquired licenses for their sales team to use salesforce.com and encouraged its employees to use it.⁵⁵

⁵³ *Brown v. Tellerate Holdings, Ltd.*, No. 2:11-cv-1122, 2014 U.S. Dist. LEXIS 90123, at *6 (S.D. Ohio July 1, 2014).

⁵⁴ *See id.* at *7, *10.

⁵⁵ *See id.* at *8.

During discovery, Tellermate contended that it could not produce the reports because, among other things, Tellermate could not “print out accurate historical records from salesforce.com”⁵⁶ Counsel for Tellermate represented to the court that “Tellermate [did] not possess or control data maintained in the salesforce.com database and [was] not at liberty to produce it in discovery,” as well as that no one from Tellermate “has access to [the] ESI of salesforce.com”⁵⁷ However, in direct contradiction from its attorneys’ representations to the court, Tellermate’s representative testified that “any Tellermate employee with a login name and a password could access . . . historical information . . . at any time.”⁵⁸

[21] Additionally, after the plaintiffs’ departure, Tellermate changed the user names to the their accounts and took no action to preserve the information in the plaintiffs’ accounts, as the data in their accounts could be changed or deleted by salesforce.com administrators at the company.⁵⁹ For the above actions, the court admonished Tellermate’s counsel, stating “all of this information was clearly known to at least some Tellermate employees since Tellermate began using salesforce.com; *had the right questions been asked of the right people, counsel would have known it as well.*”⁶⁰

[22] The court also found that “counsel apparently never identified the persons having responsibility for salesforce.com information, which would have included those Tellermate employees (named by the [plaintiffs] in their document request) whose salesforce.com accounts

⁵⁶ *Id.* at *11.

⁵⁷ *Id.* at *13.

⁵⁸ *Brown*, 2014 U.S. Dist. LEXIS 90123, at *14.

⁵⁹ *See id.*

⁶⁰ *Id.* at *19 (emphasis added).

were being requested, or the persons designated by Tellermate as its salesforce.com administrators.”⁶¹ In short, the court found that “counsel had an affirmative obligation to speak to the key players at Tellermate so that counsel and client could identify, preserve, and search the sources of discoverable information.”⁶²

[23] To competently preserve ESI, practitioners must determine the individuals who may have knowledge or information about the different issues involved in the dispute, then determine what potentially relevant documents and data those individuals have in their possession, custody, or control.⁶³ Simultaneously, practitioners should speak with their client’s information technology personnel, who can explain the company’s system-wide back up procedures, any “auto-delete” functions, and gain a general overview of where and how data resides throughout the company (e.g., e-mail servers, file share servers, VM systems, databases, etc.).⁶⁴ These steps allow a practitioner to ask the right questions of the right people in order to determine where potentially relevant information resides.

[24] Additionally, asking the right questions of the right people can also inform your decision as counsel as to what is reasonably accessible and therefore reasonably can be preserved. For example, if you learn from information technology personnel that the company’s disaster recovery systems are truly disaster recovery systems rather than a form of long-term storage, it may be worth mentioning at a FED. R. CIV. P. 26(f) conference

⁶¹ *Id.* at *52–53.

⁶² *Id.* at *56.

⁶³ See *Zubulake V*, 229 F.R.D. 422, 432 (S.D.N.Y. 2004); see also McCarroll, *supra* note 15, at 94–95.

⁶⁴ See *Zubulake V*, 229 F.R.D. at 432.

or meeting that, because these systems are for disaster recovery only, they are not reasonably accessible and will not be preserved.⁶⁵

[25] Moreover, discussing the data landscape with key custodians and information technology personnel provides valuable information about the various data sources and the amount it may cost to preserve those data sources, which can provide insight into whether producing from that data source is proportional to the needs of the case.⁶⁶ For example, in *You v. Japan* the court allowed defendant Sankei, a newspaper publisher, to modify a piece of a preservation order because of the undue burden it was placing on its business.⁶⁷ The preservation order required each party to take affirmative steps to preserve evidence related to the action by ceasing “any document destruction programs and any ongoing erasures of e-mails, voicemails, and other electronically recorded materials.”⁶⁸ Sankei took steps to comply with the order, including retaining versions of articles that it placed in a proprietary application used for laying out each edition of the newspaper.⁶⁹ The application typically retained these versions for 90

⁶⁵ See *Zubulake IV*, 220 F.R.D. 218. Amended Rule 26(f) now puts issues of preservation at the forefront of a 26(f) conference. See FED. R. CIV. P. 26(f)(3)(C) (“A discovery plan must state the parties’ views and proposals on: . . . any issues about disclosure, discovery, or preservation of electronically stored information, including the form or forms in which it should be produced . . .”) (emphasis added); see also FED. R. CIV. P. 37(e), advisory committee’s note on 2015 amendments (“A party may act reasonably by choosing a less costly form of information preservation, if it is substantially as effective as more costly forms.”).

⁶⁶ FED. R. CIV. P. 26(b)(1) (“Parties may obtain discovery regarding any nonprivileged matter that is relevant to any party’s claim or defense” and proportional to the needs of the case).

⁶⁷ See *Hee Nam You v. Japan*, No. C 15-03257 WHA, 2015 U.S. Dist. LEXIS 123877, at *2–5 (N.D. Cal. Sept. 16, 2015).

⁶⁸ *Id.* at *2.

⁶⁹ See *id.* at *2–3.

days.⁷⁰ Sankei stated that requiring that application to retain the article versions for greater than 90 days “could slow down the system or cause it to crash.”⁷¹ Sankei also stated that installing a new storage system could take up to eight months and would cost \$18 million.⁷² Accordingly, Sankei filed a motion for relief from the preservation order and proposed an alternative method to preserve the documents in the proprietary application.⁷³ The Court, noting plaintiffs’ objections, granted Sankei’s proposal and included a modification proposed by the plaintiffs.⁷⁴ Without asking the right questions of the right people, Sankei may not have been able to seek an alternative that would allow it to continue functioning as a business and maintain its preservation obligations.

B. The Litigation Hold

[26] While the litigation hold or legal hold notice should now be part of every practitioner’s litigation checklist, it is still an integral part of competently complying with the duty to preserve. As the court in *Zubulake V* stated, “[o]nce a party reasonably anticipates litigation, it must suspend its routine document retention/destruction policy and put in place a ‘litigation hold’ to ensure the preservation of relevant documents.”⁷⁵

[27] A litigation hold informs custodians and information technology personnel about the lawsuit and their preservation obligations to preserve

⁷⁰ *See id.* at *3.

⁷¹ *Id.*

⁷² *See Hee Nam You*, 2015 U.S. Dist. LEXIS 123877, at *3.

⁷³ *See id.*

⁷⁴ *See id.* at *4–5.

⁷⁵ *Zubulake V*, 229 F.R.D. at 431 (quoting *Zubulake IV*, 220 F.R.D. at 218).

potentially relevant information relating to the lawsuit.⁷⁶ However, implementing the litigation hold does not end a party's preservation obligations—"[c]ounsel [also] must oversee compliance with the litigation hold."⁷⁷

[28] *Apple Inc. v. Samsung Electronics Co., Ltd.* demonstrates the potential consequences of failing to monitor compliance with a litigation hold. There, Magistrate Judge Grewal analyzed "whether Samsung took adequate steps to avoid spoliation after it should have reasonably anticipated" litigation.⁷⁸ In this case, a Samsung entity/defendant failed to disable the "auto-delete" function of its e-mail system after the duty to preserve was triggered.⁷⁹ Judge Grewal noted that it is "generally recognized that when a company or organization has a document retention policy, it is 'obligated to suspend' that policy and 'implement a "litigation hold" to ensure the preservation of relevant documents' after the preservation duty has been triggered."⁸⁰ Samsung issued a litigation hold notice requesting employees to "preserve any and all [] documents that may be relevant to the issues in the potential litigation . . . until [the potential litigation] is fully resolved."⁸¹ However, while the litigation hold notice provided categories of documents that should be retained, Samsung took no steps to evaluate what its employees were doing to comply with the litigation hold notice, especially in light of the continued use of the

⁷⁶ *See id.* at 439.

⁷⁷ *Id.* at 432.

⁷⁸ *Apple Inc. v. Samsung Elecs. Co., Ltd.*, 881 F. Supp. 2d 1132, 1134 (N.D. Cal. 2012).

⁷⁹ *See id.* In his opinion, Judge Grewal again reiterated that the duty to preserve includes identifying, locating, and maintaining information that is relevant to the litigation. *See id.* at 1137.

⁸⁰ *Id.* at 1137 (internal citations omitted).

⁸¹ *Id.* at 1142–43.

auto-delete function.⁸² While under the legal hold, Samsung never checked to see whether a single custodian was in compliance with the given directives.⁸³

[29] Practitioners and clients should consistently monitor employee and information technology compliance with their legal hold directives. The longer a legal hold is in place and the more time that goes by opens companies up to something that can be described as “Litigation Hold Fatigue,” resulting in less enthusiastic preservation practices.⁸⁴ Additionally, as noted above, issues in a litigation change, which can change what needs to be preserved. Follow-up reminders and revisions to litigation holds not only assist in complying with preservation obligations, but they can also assist in defining the scope of preservation.

IV. WHAT CAN WE LEARN FROM FAILING TO PRESERVE

[30] Cases outlining complete failures to preserve are instructive to practitioners as a template for “Preservation Do Nots.” In *Altercare, Inc. v. Clark*, the Ohio Court of Appeals was required to determine whether the trial court abused its discretion in dismissing Altercare’s case against its former employee, Clark, for failing to preserve the former employee’s computer after the obligation to preserve arose.⁸⁵ After being told not to return to Altercare for work, Clark’s attorney sent Altercare a letter stating that it had breached Clark’s employment contract, and requesting that

⁸² See *id.* at 1145.

⁸³ See *Apple Inc.*, 881 F. Supp. 2d at 1147.

⁸⁴ See generally *Legal Hold Software*, EXTERRO, <http://www.exterro.com/e-discovery-software/legal-hold/>, archived at <https://perma.cc/HS9M-VFVQ> (last visited Feb. 20, 2016) (“Help custodians understand the importance of pending obligations, fight 'notice fatigue' by those on multiple legal holds, and promote consistent compliance.”).

⁸⁵ See *Altercare, Inc. v. Clark*, 9th Dist. No. 12CA010211, 2013-Ohio-2785, at ¶ 12.

Altercare preserve evidence relevant to the dispute.⁸⁶ The preservation notice portion of the letter provided a non-exhaustive list of data covered by Altercare’s obligation, as well as ways that Altercare could comply with its obligation.⁸⁷ Once suit was filed, Clark requested in discovery all ESI relating to Clark and/or Clark’s employment with Altercare.⁸⁸

[31] The trial court attempted to determine what Altercare did to preserve Clark’s ESI on numerous occasions.⁸⁹ The court found that, at one point, Altercare returned a different hard drive to Clark than belonged to the work computer she sent the company for preservation.⁹⁰ The trial court held that Altercare did not preserve Clark’s work computer, failing to either “[pull] it out of service or [make] a copy or clone of its hard drive at the time Ms. Clark put [Altercare] on notice” of its obligation to preserve.⁹¹ Because the trial court found that Altercare’s conduct in failing to preserve Clark’s work computer showed “such extreme carelessness and indifference,” the trial court dismissed Altercare’s complaint.⁹² The Court of Appeals affirmed the trial court’s ruling, finding that Altercare “took no action whatsoever” to preserve Clark’s computer, either when she was terminated—even though it was reasonably foreseeable that

⁸⁶ *See id.* at ¶ 2.

⁸⁷ *See id.* (“Altercare can most easily comply with its obligation by making mirror-image bit stream back-up copy of computers and storage media (such as hard disk drive[s], floppy disks, CDs, DVDs, back-up tapes, or any other electronic data), which will inexpensively preserve relevant electronic and digital evidence on searchable CD-ROMs or DVD.”).

⁸⁸ *See id.* at ¶ 3.

⁸⁹ *See id.* at ¶¶ 3–10.

⁹⁰ *See Altercare*, 2013-Ohio-2785, at ¶ 6.

⁹¹ *Id.* at ¶ 10.

⁹² *Id.*

litigation with Clark was probable—or after receiving the preservation notice from Clark’s attorney.⁹³ Notably, the Court of Appeals also recognized that the trial court “found that there was no evidence that Clark’s computer was lost as a result of a routine, good faith operation,”⁹⁴ such as a retention schedule.

[32] Similarly, in *Alter v. Rocky Point Sch. Dist.*, in ruling on the Plaintiff’s motion to compel and for sanctions in a workplace discrimination claim, the court found that defendants had failed to satisfy their duty to preserve relevant evidence.⁹⁵ The court based its ruling on the following facts:

- Defendants failed to issue a timely litigation hold, instead waiting more than two years after Plaintiff filed a Notice of Claim,⁹⁶
- Defendants “failed to discuss the litigation hold with key players” in the lawsuit,⁹⁷
- Defendants failed to inform key custodians regarding their obligation to preserve relevant evidence “on whatever devices contained the information, [including] [personal] laptops, cellphones or any personal digital devices capable of ESI storage.”⁹⁸

⁹³ *Id.* at ¶¶ 2, 16.

⁹⁴ *Id.* at ¶ 16.

⁹⁵ *See Alter v. Rocky Point Sch. Dist.*, No. 13-1100 (JS) (AKT), 2014 U.S. Dist. LEXIS 141020, at *3 (E.D.N.Y. Sept. 30, 2014).

⁹⁶ *See id.* at *28.

⁹⁷ *Id.* at *23.

⁹⁸ *Id.* *22–24, *26, *28.

[33] In *Clear-View Techs.*, discussed above, the defendants took “no reasonable steps to preserve relevant evidence” and, in fact, “affirmatively destroyed it,” after the text message that triggered the preservation obligation was sent and, in some cases, after the preservation letter was received and after suit was filed.⁹⁹

[34] In each of these cases, the party responding to destruction allegations failed to take reasonable steps to preserve potentially relevant evidence—no litigation holds issued, no custodian interviews performed or even simple questions asked, and in a workplace discrimination suit, the terminated employee’s workstation was not preserved—and was then punished in some manner by the court. As these cases demonstrate, it is this failure to competently preserve potentially relevant evidence that places clients and their attorneys on rocky ground with the court.

[35] Prior to the 2015 amendment of Rule 37(e), the sanctions imposed by courts because of the destruction of evidence, whether through negligence or bad faith, created inconsistencies in the sanctions imposed throughout the federal circuits.¹⁰⁰ In one circuit, a party could receive an adverse inference instruction from the grossly negligent deletion of an employee’s ESI,¹⁰¹ while in another, an adverse inference instruction was

⁹⁹ *Clear-View Techs., Inc. v. Rasnick*, No. 5:13-cv-02744-BLF, 2015 U.S. Dist. LEXIS 63579, at *21–23 (noting that defendants “failed to implement a hold policy,” “deleted thousands of relevant emails, [and] discarded several phones, laptops, [and] iPads...”).

¹⁰⁰ *Compare Residential Funding Corp. v. DeGeorge Fin. Corp.*, 306 F.3d 99, 108 (2nd Cir. 2002) (“The sanction of an adverse inference may be appropriate in some cases involving the negligent destruction of evidence because each party should bear the risk of its own negligence.”), *with United States v. Artero*, 121 F.3d 1256, 1259 (9th Cir. 1997) (noting that a “district judge did not abuse his discretion by refusing to give an adverse inference instruction, because the appellant showed neither bad faith imputable to the federal government nor prejudice from the loss and destruction of the evidence.”) (citing *United States v. Jennell*, 749 F.2d 1302, 1308–09 (9th Cir. 1984)).

¹⁰¹ *See Sekisui Am. Corp. v. Hart*, 945 F. Supp. 2d 494, 504 (S.D.N.Y. 2013).

appropriate only where there was a finding of bad faith in the destruction of the evidence.¹⁰² Amended Rule 37(e) no longer allows courts to punish parties through an adverse inference instruction in the wake of destroyed evidence *if* they can show they took reasonable steps to preserve evidence.¹⁰³

[36] So what does this mean for practitioners? In the words of algebra teaches everywhere, litigants must “show their work.” Litigants should document the processes by which and steps they took to preserve potentially relevant evidence. The following steps, while not all-inclusive, and when they were taken should be well-documented by practitioners:

- Issue a litigation hold that outlines the potential forms of ESI (e-mail, text messages, word documents, databases, etc.) and the potential sources of ESI (e-mail mailbox, smart phone, workstation, network servers, social media accounts, etc.) available to custodians;¹⁰⁴
- Identify and interview key players and custodians regarding their ESI forms and sources;

¹⁰² See *Rimkus Consulting Grp. v. Cammarata*, 688 F. Supp. 2d 598, 614 (S.D. Tex. 2010).

¹⁰³ See FED. R. CIV. P. 37(e) advisory committee’s note on 2015 amendments (“The rule only applies if the information was lost because the party failed to take reasonable steps to preserve the information.”).

¹⁰⁴ See generally *D.O.H. v. Lake Cent. Sch. Corp.*, No. 2:11-cv-430, 2015 U.S. Dist. LEXIS 20259, at *23–25 (N.D. Ind. Feb. 20, 2015) (discussing where custodians identify social media as a potential source of potentially relevant information, practitioners should take steps to ensure that they understand how to preserve data from a social media site or engage a third-party vendor that does understand both how the site works and how to preserve the data contained in the site.).

- Interview information technology personnel regarding forms and sources of ESI available to employees and other personnel at the company, as well as the back-up and disaster recovery systems in place;
- Document which devices were identified as having potentially relevant evidence and how each device was preserved for each custodian;
- Document how specific information on servers and other company sources was identified and preserved;
- Monitor legal hold compliance and refresh litigation hold notice as issues in the litigation evolve and new custodians are identified and new employees hired;
- Disable and document the disabling of “auto-delete” functions for systems containing such functions;
- Evaluate software offerings available to assist with the implementation of a legal hold;¹⁰⁵
- Analyze records management or retention policies for those categories of documents under a litigation hold to ensure routine destruction as to those documents has stopped.

[37] Practitioners should document what was done and when it was done to demonstrate to the court how they took reasonable steps to preserve ESI. Taking the time to identify whose data and what sources and forms of data need to be preserved, and then

¹⁰⁵ See generally Jie Zhang & Garth Landers, *Magic Quadrant for E-Discovery Software*, GARTNER (May 18, 2015), <https://www.gartner.com/doc/reprints?id=1-2G57ESF&ct=150519&st=sb>, archived at <https://perma.cc/SC7T-8DJP> (evaluating over twenty e-Discovery software vendors).

“showing your work” by documenting those preservation steps and the considerations necessary to make those choices, demonstrates competence and may save you from headaches and discord later.