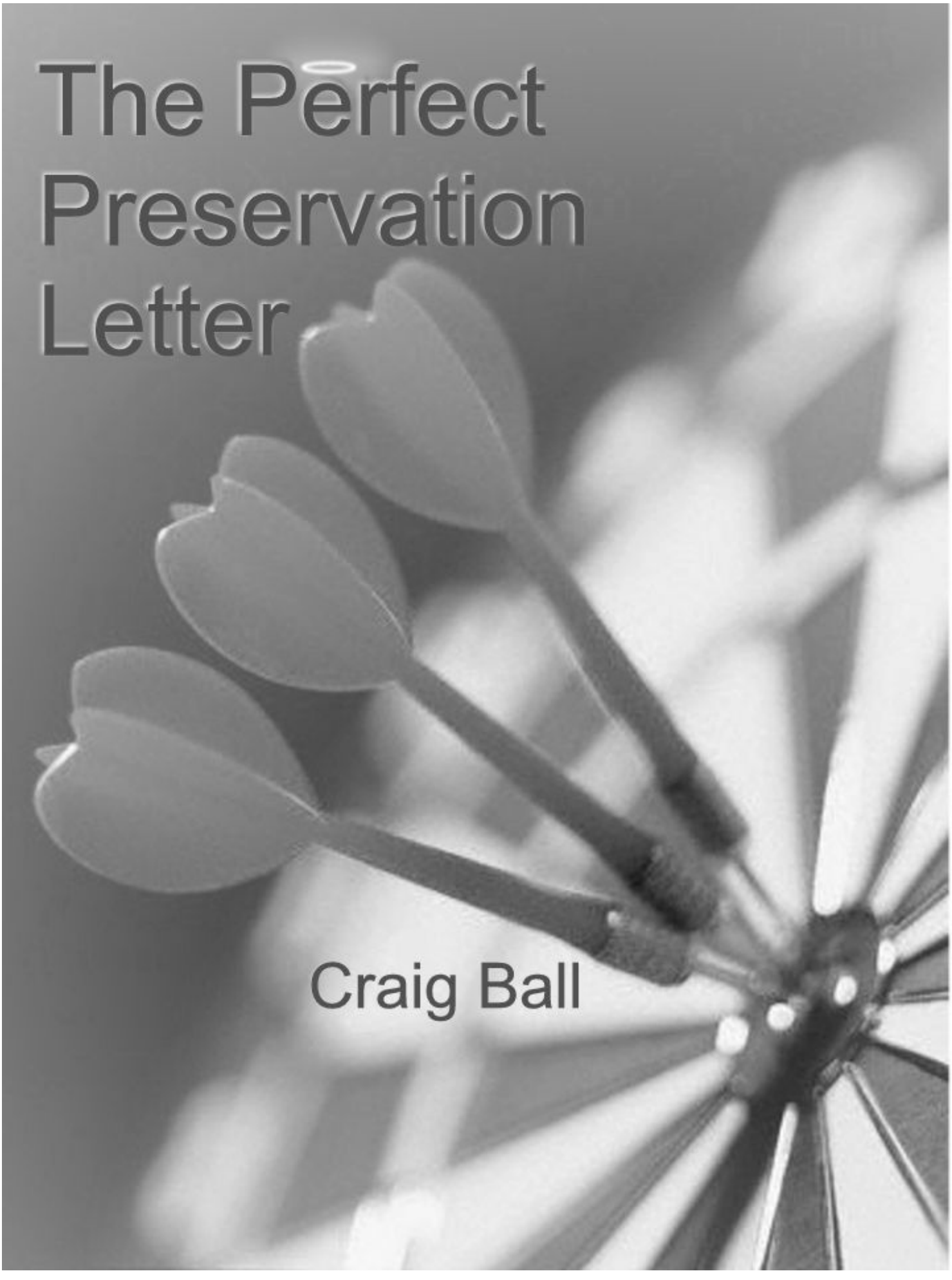
# The Perfect Preservation Letter



Craig Ball

# The Perfect Preservation Letter

**By Craig Ball**

**Well, I was drunk the day my Mom got outta prison,**
**And I went to pick her up in the rain;**
**But before I could get to the station in my pickup truck,**
**She got runned over by a damned old train.**
*From "You Never Even Called Me By My Name"*
*(a/k/a "The Perfect Country and Western Song")*
*By Steve Goodman, performed by David Allan Coe*

Outlaw musician David Allan Coe sings of how no country and western song can be "perfect" unless it talks of Mama, trains, trucks, prison and getting drunk. Likewise, no digital evidence preservation letter can be "perfect" unless it clearly identifies the materials to be retained, educates your opponent about preservation options and lays out the consequences of failing to properly preserve the data. The perfect preservation letter isn't found in a form book. It's crafted from a judicious mix of technical boilerplate and *fact-specific* direction. It compels broad retention while appearing to ask for no more than the bare essentials. It rings with reasonableness. This article discusses some features of the perfect preservation letter and offers suggestions as to how it can be effectively drafted and deployed.

**Contents**

## The Role of the Preservation Letter

> "The reality of electronic discovery is it starts off as the responsibility of those who don't understand the technology and ends up as the responsibility of those who don't understand the law."

You can read the Federal Rules of Civil Procedure from cover to cover and not see a reference to preservation letters. So why invest a lot of effort creating the perfect preservation letter? Wouldn't it be sufficient to remind your opponent that the laws and rules prohibiting destruction of evidence apply to electronically stored information in the same manner that they apply to other evidence and that they must take every reasonable step to preserve this information until the final resolution of the case? Perhaps in a decade or so it will be enough; but, today we face an explosion of electronic evidence untamed by sound records management. Too many litigators and in-house counsel are clueless about information systems. The reality of electronic discovery is it starts off as the responsibility of those who don't understand the technology and ends up as the responsibility of those who don't understand the law. A well-drafted preservation letter helps bridge this knowledge gap.

The goal of the preservation letter is, of course, to remind opponents to preserve evidence, to be sure the evidence doesn't disappear. But, the preservation letter also serves as the linchpin of a subsequent claim for spoliation, helping to establish bad faith and conscious disregard of the duty to preserve relevant evidence. It is today's clarion call that underpins tomorrow's, "I told you so." The more effectively you give notice and convey what must be retained--including methodologies for preservation and consequences of failure--the greater the likelihood your opponent will be punished for destruction of evidence.

## The Proposed Amendments to the Rules of Civil Procedure

Though serving a preservation letter isn't a formal component of civil discovery procedures, it's likely to be a *de facto* practice as federal and local rules of civil procedure impose express e-discovery "meet and confer" obligations upon litigants. For example, a proposed amendment to Rule 26 of the Federal Rules of Civil Procedure would require litigants to "discuss any issues relating to preserving discoverable information."[1] This "meet and confer" obligation springs from concerns about electronically stored information, and the preservation letter is sure to frame the agenda for such discussions.

The preservation letter will acquire still greater prominence as a result of the role it will play in a court's consideration of "safe harbor" claims by parties failing to preserve and produce electronic evidence. Two proposed amendments suggest different thresholds of misconduct supporting immunity from sanctions[2], but both turn on the subjective awareness of the party failing to

---

[1] Proposed Amendment to Rule 26(f)(2) of the Federal Rules of Civil Procedure (Report of the Civil Rules Advisory Committee, May 17, 2004, available at http://www.uscourts.gov/rules/Reports/CV5-2004.pdf)

[2] Alternative Proposed Amendments to Rule 37(f) of the Federal Rules of Civil Procedure (*Id.*):
Alternative 1:
"Unless a party violated an order in the action requiring it to preserve electronically stored information, a court may not impose sanctions on the party for failing to provide such information if: (1) the party took reasonable steps to

provide evidence. The preservation letter can establish such awareness, bolstering a claim that the party destroying evidence knew of its discoverability and recklessly or intentionally disregarded same. Per commentary to the proposed rule, "The party's sophistication in general, and with respect to electronic information systems in particular, may be relevant to this consideration."[3] A clear and instructive preservation letter that serves to educate your opponent isn't just professional courtesy; it also fosters a level of sophistication that deprives your opponent of safe harbor for misconduct based upon ignorance.

"A clear and instructive preservation letter that serves to educate your opponent isn't just professional courtesy…."

### What is Electronic Evidence Preservation?

When evidence is a paper document, preserving it is simple: We set the original or a copy aside, confident that it will come out of storage exactly as it went in. Absent disaster or tampering, the status quo is maintained. But despite lawyers' ardor for paper, 95% of information is born digitally, and the majority of that information never printed. Preserving electronic data presents its own unique challenges, such as:

- "Touching" data changes it
- Digital evidence is increasingly ill-suited to printing
- Data must be interpreted to be used
- Storage media are fragile and changing all the time
- Digital storage media are dynamic and recyclable

### Touching Data Changes It

Route a document through a dozen hands and, aside from a little finger grime or odd coffee stain, the document won't spontaneously change just by moving, copying or reading it. But open that same document in Microsoft Word, or copy it to a CD, and you've irretrievably changed that document's *metadata*, the data-about-data items like creation or last access dates that may themselves be evidence. In fact, using the Windows operating system, you *can't* copy all of a file's metadata when it's moved from hard drive to a recordable CD. The two media use different file systems such that the CD-R doesn't offer a structure capable of storing all of a file's Windows metadata.

---

preserve the information after it knew or should have known the information to be discoverable in the action; and (2) the failure resulted from loss of the information because of the routine operation of the party's electronic information system."

Alternative 2:
"A court may not impose sanctions on a party for failing to provide electronically stored information deleted or lost as a result of the routine operation of the party's electronic information system unless the deletion or loss was intentional or reckless."

[3] *Id.* Committee Note to Proposed Rule 37(f), alternative 2.

### Digital Evidence Is Increasingly Ill-Suited to Printing

Much modern evidence doesn't lend itself to paper. For example, a spreadsheet displays values derived from embedded formulae, but you can't embed those formulae in paper. In large databases, information occupies expansive grids that wouldn't fit on a printed page or make much sense if it could. And, of course, sound and video evidence can't make the leap to paper. So preserving on paper isn't always an option, and it's rarely an inexpensive proposition.

### Data Must Be Interpreted To Be Used

If legible and in a familiar language, a paper document can convey information directly to the reader. A literate person can interpret an alphabet, aided by blank space and a few punctuation marks. It's a part of our grade school "programming." But ***all*** digital data are just streams of ones and zeroes. For those streams of data to convey anything intelligible to people, the data must be interpreted by a computer using specialized programming called "applications." Without the right application—sometimes even without the correct *version* of an application—data is wholly inaccessible. Successfully preserving data also entails preserving applications capable of correctly interpreting the data as well as computing environments—hardware and software—capable of running these applications.

### Storage Media Are Fragile and Changing

If your great grandfather put a letter in a folder a century ago, chances are good that notwithstanding minor signs of age, you could pull it out today and read it. But changes in storage technology and rapid obsolescence have already rendered fifteen-year-old digital media largely inaccessible absent considerable effort and expense. How many of us still have a computer capable of reading a 5.25" floppy? The common 3.5" floppy disk is disappearing, too, with CD-ROMs fast on its heels to oblivion. Data stored on back up tapes and other magnetic and even optical media fades and disappears over time like the contents of once-common thermal fax paper. Disks expected to last a century are turning up illegible in a decade. Back up tapes stretch a bit each time they are used and are especially sensitive to poor storage conditions. Long term data preservation entails either the emergence of a more durable medium or a relentless effort to migrate and re-migrate legacy data to new media as it comes into common usage.

### Digital Storage Media Are Dynamic and Recyclable

By and large, paper is not erased and reused for information storage; at least not in a way we'd confuse its prior use as someone's Last Will & Testament with its reincarnation as a recycled cardboard carton. By contrast, a hard drive is constantly changing and recycling its contents. A later version of a document may overwrite—and by so doing, destroy—an earlier draft, and storage space released by the deletion of one file may well be re-used for storage of another. This is in sharp contrast to paper preservation, where you can save a revised printout of a document without affecting—and certainly not obliterating-- a prior printed version.

Clearly, successful preservation of digital data isn't as always as simple as copying something and sticking it in a folder; but, your opponent may be clueless about the planning and effort that digital preservation requires. In that instance, the requesting party is at a crossroads: Do you seek to educate the producing party or its counsel about how and why to properly preserve digital evidence, or do you keep mum in hopes that an advantage will flow from your opponent's

ineptitude? Most of the time, you'll want to do the former, at least until the knowledge gap shrinks and more lawyers recognize why and how to preserve digital evidence.

**The Duty to Preserve**

At what point does the duty to preserve evidence arise? When the lawsuit is filed? Upon receipt of a preservation letter? When served with a request for production?

The duty to preserve evidence may arise before—and certainly arises without—a preservation letter. In fact, the duty can arise long before an opponent takes any action. A party's obligation to preserve evidence has generally been held to arise when the party knows or has reason to know that evidence may be relevant to future litigation. This "reasonable anticipation of litigation" standard means that any person or company who should see a lawsuit on the horizon must act, *even before a preservation letter or lawsuit has materialized*, to cease activities likely to destroy electronic or tangible evidence and must take affirmative steps to preserve such evidence.

Thus, the preservation letter may be only one—albeit a decisive one--of a number of events or circumstances sufficient to trigger the duty to preserve evidence. Nevertheless, arrival of the preservation letter is often the first time responding parties focus on what evidence exists and what they will elect to save.

**Balance and Reasonableness**

The problem with preservation letters is that they often must be sent when you know little-to-nothing about your opponent's information systems; consequently, they tend to be everything-but-the-kitchen-sink requests, created without much thought given to the "how" and "how much" issues faced by the other side.

A preservation letter that demands the moon and paralyzes your opponent's operations won't be met by compliance or enforcement. Absent evidence of misconduct (such as shredding or other overt destruction of evidence), a court won't sanction a party for failing to comply with a preservation letter so onerous that no one dare turn on their computer for fear of spoliation! For a preservation letter to work, it must be reasonable on its face. Remember: all you're trying to do is keep the other side from destroying relevant evidence, and just about any judge will support you in that effort if your demands aren't cryptic, overbroad or unduly burdensome.

If it could be accomplished with paper evidence, judges expect it to be feasible with electronic evidence. Still, digital is different, and some of the ways we approach paper discovery just won't fly for electronic evidence. For example, using the term "any and all" in a request for digital evidence is a red flag for potential over breadth. Demanding that an opponent retain "any and all electronic communications" is nonsense. After all, phone conversations are electronic communications, and it's unlikely that a court would require a litigant to tape all phone calls, though a judge shouldn't hesitate to compel *retention* of the tapes *when phone calls are already recorded and relevant.* If what you want preserved is e-mail, or instant messaging or voice mail, *spell it out.* Your opponent may squawk, but at least the battle lines will be drawn over specific evidentiary items your opponent may seek to destroy instead of amorphous issues like, "What constitutes a communication?" The risk to this approach is that your opponent may fail to

preserve what you haven't specified. Still, to the extent the evidence destroyed was relevant and material, that risk may be adequately addressed by a demand to retain all information items bearing on the claims made the basis of the claim. Further, the preservation letter neither creates the duty to preserve nor constrains it. If the evidence was relevant and discoverable, then destroyed at a time when your opponent should have known to keep it, it's still spoliation.

**Preservation Essentials**

A perfect preservation letter must first and foremost seek to halt routine business practices geared to the destruction of potential evidence. Call for an end to: server back up tape rotation (as appropriate); electronic data shredding; scheduled destruction of back up media; re-imaging of drives; drive hardware exchanges; sale, gift or destruction of computer systems; and, (especially if you know computer forensics may come into play) disk defragmentation and maintenance routines. Most digital evidence disappears because of a lack of enterprise communication ("legal forgot to tell IT") or individual initiative ("this is MY e-mail and I can delete it if I want to"). So, highlight the need to effectively communicate retention obligations to those with hands-on access to systems, and suggest steps to forestall personal delete-o-thons. **Remember:** When you insist that communications about preservation obligations ***reach*** every custodian of discoverable data and that such communications stress the importance of the duty to preserve, you are demanding no more than the developing law suggests is warranted. See, e.g., *Zubulake v. UBS Warburg LLC, No. 02 Civ. 1243 (S.D.N.Y. July 20, 2004) ("Zubulake V").*

Next, get fact specific! Focus on items specifically bearing on the claim or suit--relevant business units, activities, practices, procedures, time intervals, jurisdictions, facilities and key players. Here, follow the "who, what, when, where and how" credo of good journalism. Preservation letters are more than a boilerplate form into which has been packed every synonym for document and computer in the thesaurus. If your preservation letter boils down to "save everything about anything by everyone, everywhere at any time," it's time to re-draft it because not only will no trial court enforce it, many will see it as discovery abuse.

The preservation letter's leading role is to educate your opponent about the varieties of relevant electronic evidence which may exist and the importance of taking prompt, affirmative steps to be sure that evidence remains accessible. Educating the other side isn't a noble undertaking—it's sound strategy. Spoliation is frequently defended on the basis of ignorance; *e.g.,* "Your honor, we had no idea that we needed to do that," and your goal is to slam the door hard on the "it was an oversight" excuse. Doing so entails more than just reciting a litany of storage media to be preserved.

Finally, don't be so focused on electronic evidence that you fail to direct your opponent to retain the old-fashioned paper variety. Also, don't compel your opponent to preserve data to an extent much greater than *your* client could sustain. Doing so could hurt your credibility with the court right out of the gate.

**The Nature of the Case**

Formal discovery requests necessarily follow the service of a complaint or petition, so the parties have some idea what the dispute is about by the time the discovery request arrives. A pre-suit preservation letter, on the other hand, may be your opponent's first inkling that they are

facing litigation. Don't just assume that the people receiving the preservation letter know what the dispute is about; instead, *spell it out for them*. Though you may be unprepared to draft your formal complaint, you must nonetheless furnish sufficient information about the nature of the case to sustain a later claim that a reasonable person reading the preservation letter should have known to preserve particular evidence. Names of key players, dates, business units, office locations and events will all be weighed in deciding what's relevant and must be retained. The more you can offer, the less likely you are to someday hear, "If you wanted Bob's e-mail, why didn't you name Bob in the preservation letter?"

**When to Send a Preservation Letter**

"There may be circumstances where you ***want*** your opponent's routine destruction of information to continue…."

The conventional wisdom is that preservation letters should go out immediately; that is, as soon as you can identify the potential defendants. But there may be compelling reasons to delay sending a preservation letter. For example, when you face opponents who won't hesitate to intentionally destroy evidence, your preservation letter may serve as the starting gun and blueprint for their delete-o-thon. Instead, consider seeking a temporary restraining order or the appointment of a special master. Another case for delay occurs when your investigation is ongoing and the service of a preservation letter will cause opposing counsel to be engaged and trigger privileges running from the anticipation of litigation. And of course, there may be circumstances where you ***want*** your opponent's routine destruction of information to continue, such as where information unfavorable to your position will be discarded by your opponent in the usual course of business.

**Who Gets the Letter?**

If a lawsuit hasn't been filed and counsel has not appeared for your opponent, to whom should you direct your perfect preservation letter? Here, the best advice is to err on the side of as many appropriate persons as possible. Certainly, if an individual will be the target of the action, he or she should receive the preservation letter; however, if you know of others who may hold potential evidence (such as the defendant's spouse, accountant, employer, banker, customers and business associates), it may be wise to serve a preservation demand upon them making clear that you are also seeking preservation of physical and electronic records in their possession pertaining to the matters made the basis of the contemplated action. Some litigants use the preservation letter as a means to put pressure upon customers lost to, or being solicited by, a competitor-defendant. ***Beware***…as the preservation letter isn't a discovery mechanism expressly countenanced by the rules of procedure, its use as an instrument of intimidation may not be privileged and could provoke a counterclaim based on libel or tortuous interference.

If the potential defendant is a corporation, a presentation addressed to the wrong person in the organization may be ignored or delayed in reaching those empowered to place a litigation hold on records. Consequently, it's wise to direct preservation letters to several persons within the organization, including, *inter alia*, the Chief Executive Officer, General Counsel, Director of Information Technologies and perhaps even the Head of Corporate Security and the registered agent for service of process. You may also want to direct a copy to other departments, facilities or business units. You naturally want to be sure that as many who hold evidence as possible

are put on notice, but you also want to disseminate the preservation duty widely to foment uncertainty in those who might destroy evidence but for the possibility that others in the organization will retain copies. Of course, if counsel has entered an appearance, weigh whether you are constrained from communicating directly with represented parties.

If possible, consider who is most likely to *unwittingly* destroy evidence and be certain that person receives a preservation letter. Sending a preservation letter to a person likely to destroy evidence ***intentionally*** is a different story. The letter may operate as the triggering event to a delete-o-thon, so you may need to balance the desire to give notice against the potential for irretrievable destruction.

Of course, preservation letters, like any important notice, should be dispatched in a way enabling you to prove receipt, like certified mail, return receipt requested.

### How *Many* Preservation Letters?

Turning to the obligatory litigation-as-war metaphor, is a preservation letter best delivered as a single giant salvo across the bow of your opponent's armada, or might it instead be more effectively launched as several carefully-aimed shots? The common practice is to dispatch an all-inclusive request, but might it be smarter to draft your preservation demand as a series of focused requests, broken out by, *e.g.*, type of digital medium, issues, business units, or key players? Your preservation letter is destined to be an exhibit to a motion, so when the time comes to seek sanctions for a failure to preserve evidence, wouldn't it be more compelling to direct the court to a lean, specific preservation notice than to ¶ 27(c)(7)(i) of a bloated beast? Also, consider supplementing a "master" preservation notice with specific notices directed at key players. It's difficult to claim, "We didn't realize you wanted ***Bob's*** e-mail" when Bob got his very own, custom-tailored preservation letter.

## Specifying Form of Preservation

The proposed amendments to the Federal Rules of Civil Procedure would permit a requesting party to specify the form in which the requesting party wants electronic evidence to be produced. Some states, notably Texas, already permit such a designation in the rules governing discovery. Sometimes, there's no additional trouble or expense for the producing party to generate one format versus another. A non-native production format may even prove easier or cheaper to manage. But, should the *preservation letter* specify the form in which the data should be preserved? Generally, the answer is "No," because you don't want your preservation letter to appear to demand anything more onerous than maintaining evidence in the way it's kept in the ordinary course of business. On the other hand, when your specification operates to ***ease*** the cost or burden to the producing party or otherwise ***helps*** the producing party fulfill that party's preservation obligation, a format should be *suggested* (although, be clear that the specified form is just one acceptable format).

## Special Cases: Back Up Tapes, Computer Forensics and Metadata

The e-discovery wars rage in the mountains of e-mail and flatlands of Excel spreadsheets, but nowhere is the battle so pitched as at the front lines and flanks called *back up tapes, computer forensics and metadata*. These account for much of the bloodshed and so deserve special consideration in a preservation letter.

### Back Up Tapes

In the "capture the flag" e-discovery conflicts now waged, the primary objective is often your opponent's server back up tapes or, more particularly, forcing their retention and restoration. Back up systems have but one legitimate purpose, being the retention of data required to get a business information system "back up" on its feet in the event of disaster. To this end, a business really only needs a narrow look back interval since there are few instances where a business wants to re-populate its information systems with stale data. Because only the latest data has much utility in a properly designed back up system, the tapes containing the oldest backed-up information are typically recycled after a period of time to hold newer information. This practice is called "tape rotation," and the interval between use and reuse of a particular tape or set of tapes is the "rotation cycle."

Ideally, the contents of a back up system should be cumulative of the active "online" data found on the servers, but because businesses have entrusted the power and opportunity to destroy data to virtually every person in the organization (including those motivated to make data disappear), back up tapes are often the only means to preserve evidence that lies beyond the ambit of those with an incentive to destroy it. If we reach back as far as Col. Oliver North's deletion of e-mail subject to subpoena in the Iran-Contra affair, it was the government's back up system that gave up the (literally) "smoking gun" evidence.

Another reason back up tapes lie at the epicenter of e-discovery disputes is that many organizations elect to retain back up tapes for archival purposes (or in response to litigation hold instructions) long after they've lost their usefulness for disaster recovery. Here again, when data has been deleted from the active systems, the stale back up tapes are a means (joined by, *inter alia*, computer forensics and discovery from local hard drives) by which the missing pieces of the evidentiary puzzle can be restored.

In large organizations with many servers, back up systems are complex, hydra-headed colossi. There may be no simple one-to-one correspondence between a single server and a particular user, and most tape back up systems structure stored data differently from the way it resided on the server, complicating its restoration and exploration. Volume, complexity and the greater time it takes to access tape compared to disk all contribute to the high cost of targeting back up tapes in discovery. Compelling a large organization to interrupt its tape rotation, set aside back up tapes and purchase a fresh set can carry a princely price tag, but if the tapes aren't preserved, deleted data may be gone forever. This is the Hobson's choice[4] of e-discovery.

A preservation letter should target just the back up tapes that are likely to contain deleted data relevant to the issues in the case—a feat easier said than done. Whether by Internet research, contact with former employees or consultation with other lawyers who've plowed the same ground, seek to learn all you can about the architecture of the target active and back up systems. Though you may not learn much, the effort may allow a more narrowly-tailored preservation request or justify a very broad one.

[4] Thomas Hobson was a British stable keeper in the mid-1600s whose policy was that you either took the horse nearest the stable door or he wouldn't rent you a horse. "Hobson's choice" has come to mean an illusory alternative. Back up tapes are problematic, but the unacceptable alternative is letting evidence disappear.

The responding party need not retain purely cumulative evidence, so once it can be established that data has not been deleted and all relevant information still exists on the servers, the back up tapes should be released to the rotation. Again, this is a goal more easily described than achieved because it requires three elements too often absent from the adversarial process: ***communication, cooperation and trust*.** Hopefully, the advent of compulsory meet-and-confer sessions will force litigants to focus on e-discovery issues sufficiently early to stem unnecessary costs by narrowing the breadth of preservation efforts to just those actions or items most likely to yield discoverable data.

**Drive Cloning and Imaging**

When data is deleted from a personal computer, it's not gone. The operating system simply releases the space the data occupies for reuse and treats the space as empty. The data is rarely erased as part of the deletion process. In fact, there are three ***and only three*** ways that information can truly be erased from a personal computer:

1. Overwriting the places where the deleted data resided on the magnetic media (*e.g.,* floppy disk, tape or hard drive) with new information;
2. Strongly encrypting the data and then "losing" the encryption key; or,
3. Physically destroying the magnetic media such that it cannot be read.

There are three ***and only three*** ways that information can truly be erased from a personal computer

Computer Forensics is the name of the science that pursues resurrection of deleted data from storage media by processes that typically entail analysis of every region of the source media. Because operating systems turn a blind eye to deleted data (or at least that which has gone beyond the realm of the Recycle Bin), a copy of a drive made by ordinary processes won't duplicate deleted data. Computer forensic scientists use specialized tools and techniques to copy every sector on a drive, including those containing deleted data. When this stream of data containing each bit on the media (hence the term "bitstream") is duplicated to another drive, the resulting forensically-qualified duplicate is called a "clone." When the bitstream is stored in a file, the file is called a "drive image." Computer forensic tools are specially designed to analyze and extract data from both clones and images.

In routine computer operation, deleted data will be overwritten by random re-use of the space it occupies and by system maintenance activities; consequently, the ability to resurrect deleted data with computer forensics erodes over time. When the potential for discovery from deleted files on personal computers is an issue, a preservation letter may specify that the computers on which the deleted data reside should either be removed from service and shut down or imaged in a forensically-competent manner. Such a directive might read:

> You are obliged to take affirmative steps to prevent anyone with access to your data, systems and archives from seeking to modify, destroy or hide electronic evidence on network or local hard drives (such as by deleting or overwriting files, using data shredding and overwriting applications, defragmentation, re-imaging or replacing drives, encryption, compression, steganography or the like). With

> respect to local hard drives, one way to protect existing data on local hard drives is by the creation and authentication of a forensically-qualified image of all sectors of the drive. Such a forensically-qualified duplicate may also be called a bitstream image or clone of the drive. Be advised that a conventional back up of a hard drive is not a forensically-qualified image because it only captures live data files and fails to preserve forensically-significant data that may exist in such areas as unallocated space, slack spaces and the swap file. With respect to the hard drives and storage devices of each persons named below and of each person acting in the capacity or holding the job title named below, as well as each other person likely to have information pertaining to the instant action on their computer hard drive(s), demand is made that you immediately obtain, authenticate and preserve forensically-qualified images of the hard drives in any computer system (including portable and home computers) used by that person during the period from ____ to _____, as well as recording and preserving the system time and date of each such computer.
>
> [Insert names, job descriptions and titles here].
>
> Once obtained, each such forensically-qualified image should be labeled to identify the date of acquisition, the person or entity creating the image and the system from which it was obtained. Each such image should be preserved without alteration.
>
> **Be advised that booting a drive, examining its contents or running any application will irretrievably alter the evidence it contains and may constitute unlawful spoliation of evidence.**

**Metadata**

Metadata, the "data about data" created by computer operating systems and applications, may be critical evidence in your case, and its preservation requires prompt and definite action. Information stored and transmitted electronically must be tracked by the system which stores it and often by the application that creates it.

For example, a Microsoft Word document is comprised of information you can see (*e.g.,* the text of the document and the data revealed when you look at the document's "Properties" in the File menu), as well as information you can't see (*e.g.*, tracked changes, revision histories and other data the program uses internally). This application metadata is stored inside of the document file and moves with the file when it is copied or transmitted. In contrast, the computer system on which the document resides keeps a record of when the file was created, accessed and modified, as well as the size, name and location of the file. This system metadata is typically not stored within the document, at least not completely. So when a file is copied or transmitted—as when burned to disk for production—its potentially relevant and discoverable system metadata is not preserved or produced. Worse, each time someone looks at the document or copies it, the metadata can be irreparably altered. Unless steps are taken to preserve metadata, it can be corrupted by something as common as a virus scan.

Metadata is not a critical element in all disputes, but in some the issue of ***when*** a document or record was created, altered or copied lies at the very heart of the matter. If you reasonably anticipate that metadata will be important, it is ***essential*** to make the producing party aware of the need to preserve it and the risks that threaten its corruption. Because many aren't aware of metadata—and even those who are may think of it just in the context of application metadata—the preservation letter needs to define metadata and educate your opponent about where to find it, the common operations that damage it and, if possible, means by which it can be preserved.

## End Game

Are you prepared to let relevant evidence disappear without a fight? ***No!***
Can the perfect preservation letter really make *that* much difference? ***Yes!***

The preservation letter demands your best effort for a host of reasons. It's the basis of your opponent's first impression of you and your case. A well-drafted preservation letter speaks volumes about your savvy, focus and preparation. An ill-drafted, scattergun missive suggests a form book attorney who's given little thought to where the case is going, while a letter that demonstrates close attention to detail and preemptively slams the door on cost-shifting and "innocent" spoliation bespeaks a force to be reckoned with. The carefully-crafted preservation letter serve as a blueprint for meet and confer sessions and a touchstone for efforts to remedy destruction of evidence.

Strategically, the preservation letter forces your opponent to weigh potential costs and business disruption at the outset, often before a lawsuit is filed. If it triggers a litigation hold, everyone from the board room to the mail room may learn of the claim and be obliged to take immediate action. It may serve as the starting gun for a reckless delete-o-thon or trigger a move toward amicable resolution. But done right, ***the one thing it won't be is ignored*****.**