

Ball

3

on

EDD



Three Articles on Electronic Data Discovery

Discovery of Electronic Mail: The Path to Production  
The Plaintiffs' Practical Guide to E-Discovery  
The Perfect Preservation Letter

Craig Ball

© 2005



# Three on EDD

## Three Articles on Electronic Data Discovery

Everyone uses computers—at home, at work, on the road, leaving voicemail, opening card key doors--everywhere, every day. Nearly all documentary evidence is created digitally, and only about a third or less gets printed out. As lawyers, we're duty bound to zealously pursue the truth, so we can't walk away from 2/3rds of the evidence or turn a blind eye to its metadata. We must master electronic discovery and learn to exploit its power to bring the best evidence to the decision maker in the most cost-effective way.

These three articles offer practical strategies geared to helping you succeed in your use of electronic discovery.

### Contents:

#### **1. Discovery of Electronic Mail: The Path to Production** **p. 3**

This article outlines issues and tasks faced in production of electronic mail—certainly the most common and perhaps the trickiest undertaking in electronic discovery. It's a guide to aid attorneys meeting and conferring with opposing counsel, working with e-discovery service providers, drafting production requests and explaining the cost and complexity of e-mail production to clients and the court.

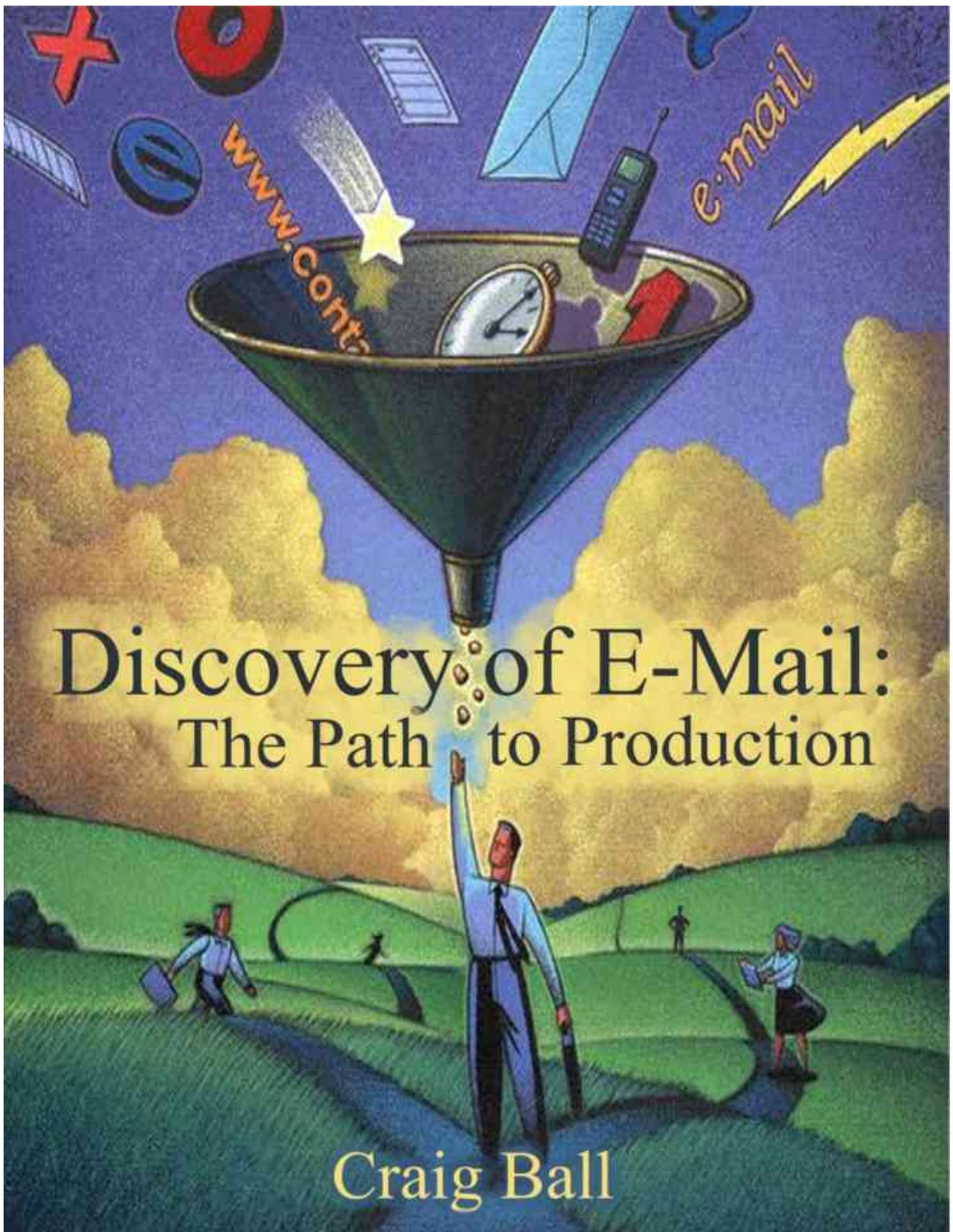
#### **2. The Plaintiff's Practical Guide to E-Discovery** **p. 12**

This two part article focuses on the needs of the requesting party. Part I addresses challenges unique to EDD, elements of a successful e-discovery effort and steps to compel preservation of digital evidence. Part II looks at the pros and cons of production formats and explores common e-mail systems, concluding with tips for getting the most out of your e-discovery efforts and budget.

#### **3. The Perfect Preservation Letter** **p. 34**

This article takes a close look at what is usually the requesting party's first foray into EDD: the letter demanding that electronic evidence be preserved. A properly drafted preservation letter can serve as the e-discovery blueprint for the case, and the considerations that go into drafting the "perfect" preservation letter reveal much about the power and challenges of EDD.

#### **About the Author** **p. 47**



## Discovery of Electronic Mail: The Path to Production

Asked, “Is sex dirty,” Woody Allen quipped, “Only if it’s done right.” That’s electronic discovery: if it’s ridiculously expensive, enormously complicated and everyone’s lost sight of the merits of the case, you can be pretty sure you’re doing it right.

But it doesn’t *have* to be that way.

This article outlines issues and tasks faced in production of electronic mail—certainly the most common and perhaps the trickiest undertaking in electronic discovery. It’s a guide to aid attorneys meeting and conferring with opposing counsel, working with e-discovery service providers, drafting production requests and explaining the cost and complexity of e-mail production to clients and the court. It offers no short cuts, but that’s not the point. The goal is to keep you from stepping off a cliff. Not every point outlined here is suited to every production effort, but all deserve *consideration* every time.

### Think Ahead

False starts and missteps in electronic discovery are painfully expensive, or even unredeemable if data has been lost. One way to avoid re-treading ground is to question expectations from the outset.

*Will the data produced:*

- *Integrate paper and electronic evidence?*
- *Be electronically searchable?*
- *Preserve all relevant metadata from the host environment?*
- *Be viewable and searchable using a single application?*
- *Be Bates numbered, and by what method?*
- *Be easily authenticable for admission into evidence?*

After attorney review, data harvest is byte-for-byte the costliest phase of electronic discovery. Understandably, producing parties want to search once and be done with it and confine the requesting party to a single list of keywords. From the requesting party’s perspective, it’s often impossible to frame effective keyword searches absent familiarity with the argot used to describe the events and objects central to the case, resulting in keyword searching missing what well-trained reviewers would find.

Producing parties are often forced to return to the well. Where you anticipate that new keywords will emerge or different search techniques will be used, securing the least costly outcome warrants the most expensive beginning: compiling a comprehensive review set of all potentially relevant e-mail. This entails *identification, preservation, harvest and population*.

### Identification

“*Where’s the e-mail?*” It’s a simple question, but one answered too simply—and erroneously--by, “It’s on the e-mail server” or “The last sixty days of mail is on the server and the rest is purged.” Certainly some of the e-mail will reside on the server, but just as certainly more, even *most*, e-mail is elsewhere, and it’s *never all gone* notwithstanding retention policies dictating it disappear. The true location and extent of the e-mail depends on systems configuration, user habits, back up procedures and other hardware, software and behavioral factors. This is true for mom-and-pop shops, for large enterprises and for everything in-between.

*How thorough is your effort to identify e-mail?* E-mail resides in some or all of the following venues, grouped according to relative accessibility:

Easily Accessible:

- Online e-mail residing in active files on enterprise servers  
*MS Exchange e.g., (.EDB, .STM, .LOG files)*  
*Lotus Notes (.NSF files)*  
*Novell GroupWise (.DB files)*
- E-mail stored in active files on local or external hard drives and network shares  
*User workstation hard drives (e.g., .PST, .OST files for Outlook and .NSF for Lotus Notes)*  
*Laptops (same as above)*  
*“Local” e-mail data files stored on networked file servers (“network shares”)*  
*Mobile devices (PDA, “smart” phones, Blackberry)*  
*Home systems, particularly those with remote access to office networks*
- Nearline e-mail  
*Optical “juke box” devices*  
*Back ups of individual users’ e-mail folders (i.e., “brick-level” back ups)*
- Offline e-mail stored in networked repositories  
*e.g., Zantaz EAS®, EMC EmailXtender®, Waterford MailMeter Forensic®*

Accessible, but Often Overlooked:

- E-mail residing on remote servers  
*ISPs (IMAP, POP, HTTP servers), Gmail, Yahoo Mail, Hotmail, etc.*
- E-mail forwarded and carbon copied to third-party systems  
*Employee forwards e-mail to self at personal email account*
- E-mail threaded behind subsequent exchanges  
*Subject and latest contents diverge from earlier exchanges lodged in body of email*
- Offline local e-mail stored on removable media  
*External hard drives, thumb drives and memory cards*  
*Optical media: CD-R/RW, DVD-R/RW*  
*Floppy Drives, Zip Drives*
- Archived e-mail  
*Auto-archived to additional .PST by Outlook or saved under user-selected filename*
- Common user “flubs”  
*Users experimenting with export features unwittingly create e-mail archives*
- Legacy e-mail  
*Users migrate from e-mail clients “abandoning” former e-mail stores*
- E-mail saved to other formats  
*.pdf, .tiff, .txt, .eml, etc.*
- E-mail contained in review sets assembled for other litigation/compliance purposes
- E-mail retained by vendors or third-parties (e.g., former service provider)
- Print outs to paper

More Difficult to Access:

- Offline e-mail on server back up media  
*Back up tapes (e.g., DLT, AIT)*
- E-mail in forensically accessible areas of local hard drives  
*Deleted e-mail*  
*Internet cache*  
*Unallocated clusters*

The issues in the case, key players, relevant times, agreements between the parties and orders of the court determine the extent to which locations must be examined; however, the failure to *identify* all relevant e-mail carries such peril that caution should be the watchword. Isn't it wiser to invest more to know *exactly* what the client has than concede at the sanctions hearing the client failed to preserve and produce evidence it didn't know it had because *no one bothered to look for it?*

### Preservation

The duty to preserve potentially relevant evidence is generally triggered by the anticipation of a claim. Fulfilling a preservation duty with respect to e-mail is made harder by the control reposed in individual users, who establish quirky folder structures, commingle personal and business communications and—most dangerous of all—control deletion and retention of their messages. Although individual users should be directed to retain all potentially relevant messages and *regularly* furnished *sufficient* information to assess relevance *consistently*, the potential for human frailty shouldn't be overlooked. *Don't leave the fox guarding the henhouse.* Act promptly to protect data from spoliation at the hands of users most inclined to sweep it under the rug.

Consider the following as parts of an effective e-mail preservation effort:

- Litigation hold notices to users, including clear, practical and specific retention directives  
*Notices should remind users of relevant places where their email may reside*  
*Be sure to provide for notification to new hires and collection from departing employees*
- Suspension of “retention” policies that call for purging email
- Suspension of re-use (“rotation”) of back up media containing email
- Suspension of hardware and software changes which make email inaccessible  
*Replacing back up systems without retaining the means to read older media*  
*Re-tasking or re-imaging systems for new users*  
*Selling, giving away or otherwise disposing of systems and media*
- Preventing users from deleting/altering/corrupting email  
*Immediate and periodic “snapshots” of relevant user email accounts*  
*Modifying user privileges settings on local systems and networks*  
*Archival by auto-forwarding selected e-mail traffic to protected storage*
- Restricting activity—like moving or copying files—tending to irreparably alter file metadata
- Packet capture of Instant Messaging (IM) traffic or *effective* enforcement of IM prohibition
- Preserve potential for forensic recovery  
*Imaging of key hard drives or sequestering systems*  
*Suspension of defragmentation*  
*Barring use of wiping software and encryption, with audit and enforcement*

A threshold issue is whether there exists a duty of preservation going forward, e.g., with respect to information created during the pendency of the action. If not, timely harvest of data, imaging of drives and culling of relevant back ups from rotation (to name a few) may sufficiently satisfy the preservation duty so as to allow machines to be re-tasked, systems upgraded and back up tape rotation re-initiated. Seeking guidance from the court and working with opposing counsel to craft a preservation order help to insulate a producing party acting in good faith from subsequent claims of spoliation.

### Harvest

Knowing what e-mail exists and where, and having taken proper steps to preserve it, it's time to gather potentially relevant messages and attachments into a **comprehensive review** set or select and assemble

responsive items into a **preliminary production** set. The difference between the two is that a comprehensive review set is compiled largely without regard to what information will be selected for production. It's a "kitchen sink" assemblage, though ultimately its scope is constrained by the business units, facilities, machines and media selected for examination. By contrast, a preliminary production set is comprised of only those e-mails and attachments that the persons collecting the data from the various files and machines deem responsive to the production requests. When a corporate defendant relies upon each employee to locate and segregate responsive e-mails or when a legal assistant goes from office-to-office selecting e-mails, the resulting collection is a preliminary production set.

The principal advantage of selective harvest is that it cuts the number of messages and attachments subject to attorney review, reducing short run cost. These savings come with attendant risks, among them the need to return to every machine if the initial harvest proves insufficient, the much greater potential for loss or corruption of overlooked evidence and inconsistencies between reviewer judgments. Also, if keyword or concept searches are employed to select e-mail for harvest, be sure to weigh the concerns about such techniques that are discussed later in this article.

The advantage of a comprehensive review set is that despite a larger initial outlay, as new requests and issues arise, the comprehensive collection can be culled again-and-again at little incremental expense. Moreover, by broadly preserving e-mail, a comprehensive review set is a valuable hedge against spoliation claims. For entities subject to ongoing litigation and compliance production, such a comprehensive collection may also be availing in multiple matters.

Whichever method is used, special care must be taken during data harvest to preserve the integrity of the evidence. It's essential to maintain a sound *chain of custody* for harvested data and be able to establish the *origin* of the e-mail (e.g., system, user account, folder and file from which it was collected) as well as the *custodian* of the e-mail. It's critical to understand that there is more to an e-mail than what a client application like Microsoft Outlook or Lotus Notes displays onscreen. When authenticity is challenged, the unseen header information or encoded attachment data is needed. Accordingly, select a harvest method that preserves *all of the data* in the e-mail.

Another chain of custody requirement is the ability to demonstrate that no one tampered with the data *between* the time of harvest and its use in court. Testimony of the custodians about handling and storage is one solution. Better still, cryptographic hashing, a form of digital "fingerprinting" applied to sections of each e-mail and attachments, generates a alphanumeric value that can be archived with the evidence and used to conclusively establish data integrity, if challenged.

Finally, there is also even more to an e-mail than its contents because, as is true of every file stored on a computer, there is associated *metadata* (data *about* data). Each email must be tracked and indexed by the e-mail client application ("application metadata") and every file containing the e-mail must be tracked and indexed by the file system of the computer storing the data ("system metadata"). E-mail metadata can be important evidence in its own right, helping to establish, e.g., whether or when a message was received, read, forwarded, changed or deleted. System metadata is particularly fragile since most computer users think themselves fully capable of copying a file from one medium to another and fail to appreciate that simply copying a file from a hard drive to a floppy *changes the file's metadata* and potentially destroys critical evidence. Select your methods carefully to insure that the act of harvesting data as evidence doesn't alter the evidence or its metadata. If method chosen alters metadata, *archive the correct metadata before it changes*. Though cumbersome, a spreadsheet reflecting the original metadata is preferable to spoliation. Electronic discovery and computer forensics experts can recommend approaches to resolve these and other data harvest issues.

## Population

Your scrupulous e-mail harvest is complete, but what you've reaped is no more ready to be searched for evidence than wheat is fit to be a sandwich. Harvested data arrives in varying incompatible formats on different media. Expect massive database files pulled from Microsoft Exchange and Lotus Domino Servers, .PST and .NSF files copied from local hard drives, HTML pages of browser-based e-mail, paper printouts, .PDF and .TIFF images (some searchable, some not) and all manner of forms and formats described in the Identification section, above. Were you to dump it all on a big hard drive and try to view it or run keyword searches, you'd quickly discover it yields up little information. That's because most of the data isn't stored as text. Some of it is locked up (password protected), some encrypted (e.g., Lotus Notes files) and some compressed, which frustrates text searching as effectively as encryption. The scanned data is a picture, not text, and the e-mail attachments are encoded in a hieroglyphic called "Base 64."

Before search tools and reviewers can do their jobs, the harvested data must be deciphered and reconstituted to be accessible and re-appear as the *words* we see when using e-mail clients and word processors. This is accomplished by, for example,

- Opening password protected files
- Decrypting container files and items (e.g., Lotus Notes .NSF)
- Decompressing email container files (e.g., Outlook .PST, .EBD, .OST)
- Converting attachments to compatible formats (e.g., Base64, MIME)
- Decompressing and decrypting attachments (e.g., .ZIP, .XLS, )
- Optical character recognition of document image attachments (e.g., .TIFF)
- Identifying Unicode-formatted and foreign language attachments and documents (e.g., .DOC)
- Accessing files in obscure or proprietary formats
- Repairing corrupted files

By this point, decisions must be made as to what media and methods will be used to host and review the data. Will counsel for the producing party pore over CDs, DVDs or portable hard drives or wade through network attached storage or online repositories? The assembled data should be organized to make it possible to pair the e-mail with its metadata and to trace messages and attachments back to their origins, by, e.g., custodian, interval, location, business unit or other taxonomy.

## De-duplication

You *finally* made it. The e-mails are assembled, accessible and intelligible. You *could* begin your review right away, but unless your client has money to burn, there's one more thing to do before diving in: *de-duplication*. If Jane e-mails Tom, with copies to Dick and Harry and Tom responds with an attachment by clicking "Reply to All," Tom's response is in *both* Tom's Sent Items folder *and* his Inbox, as well as in Jane, Dick and Harry's Inboxes. Save for variations in time of receipt, the messages are functionally identical. Absent de-duplication, Tom's response will be reviewed five times. Not only is this a costly waste of time, it creates the potential for conflicting decisions respecting relevance and privilege issues. The better course would be to use specialized software to remove all but a single instance of Tom's response from the review set.

De-duplication is typically achieved using metadata, cryptographic hashing or a mix of the two. It may be implemented *vertically*, within a single mailbox, folder or custodian, or *horizontally* (also called *globally*) across multiple mailboxes and multiple custodians. It's essential to *track and log all de-duplication* to permit re-population of duplicated items to be produced.

Be careful with horizontal de-duplication as discovery strategies change. An e-mail sent to dozens of recipients may have been de-duplicated from all but one custodian's mailbox in the expectation that the message would be reviewed and a production decision made on review of that single mailbox. If that custodian's e-mail is excluded from review, the de-duplicated e-mail is *never* reviewed, even if all other custodian's mailboxes are examined. Here, de-duplication could result in the failure to produce a discoverable document.

### **Review**

At last, you and your staff are looking at the e-mail to flag:

- Relevant, discoverable and non-privileged items
- Items responsive to particular requests
- Privileged communications (attorney-client, doctor-patient, work product)
- Confidential communications (trade secrets, proprietary data, personal and private)

If the review set is large, counsel may employ keyword or concept search tools to identify privileged or responsive items. Though a cost effective approach and useful when responding to objective requests (e.g., "produce all e-mail between Jane and Tom"), the value of automated search tools is considerably less clear when used to process subjective requests (e.g., "produce all e-mail expressing product safety concerns."). As previously noted, it's often impossible to frame effective keyword searches absent familiarity with the lingo used to describe the events and objects central to the case. Even then, the crucial communiqué, "*Say nothing*" or "*Dump her*" may be overlooked.

Properly used by those who understand their strengths and recognize their limitations, text and concept search tools are an important adjunct to—but an inadequate substitute for—the judgment of a diligent, well-trained reviewer. If you use automated search tools, be prepared to demonstrate to the court and opposing counsel how such tools compare with the efficacy of human reviewers and the basis for such comparison. Know that in the only litigation study comparing the two this author has found, keyword searching fared poorly, finding only about one-fifth of the relevant items identified by human reviewers. The safest approach is to work cooperatively with opposing counsel to select the keywords and frame the searches to be run against the review set. Mailboxes of key witnesses *always* merit careful message-by-message review for relevant intervals.

### **Re-population**

Once it's been decided what to produce and withhold, the production set should be re-populated with all relevant and discoverable non-privileged messages and attachments that were de-duplicated for review. Alternatively, discuss the issue with opposing counsel and determine counsel's preference. Counsel for the requesting party may be satisfied with a log detailing other recipients, if it serves to simplify his review without causing undue confusion. Don't produce de-duplicated e-mail without establishing and memorializing that opposing counsel knows of the de-duplication and waives re-population.

### **Redaction**

When a paper record held discoverable and privileged content, the time-honored solution was to conceal the privileged text with heavy black marking pen and produce a photocopy of the redacted original. Shortsighted efforts to carry that practice into the realm of electronic discovery proved embarrassing when it was discovered that simply obscuring text on the image layer of, e.g., a document file in Adobe Portable Document Format (.PDF) did nothing to conceal the same text in the file's data layer. Electronic

evidence demands different methods to remove privileged and confidential information from discoverable items. Any method employed must eradicate redacted data from all source data including:

- MIME/UU/BASE64 encoded attachments
  - All e-mails are plain text file, yet we use them to transport photos, music, programs and all manner of binary files as “attachments”. In truth, non-text data aren’t “attached” at all. Thanks to an encoding scheme called Base64, binary data hitch a ride, embedded within the body of the e-mail, masquerading as text. If an attachment contains privileged content, know that producing the complete contents of the e-mail (that is, not just the message but the file’s headers and footers, too) enables the privileged content to be decoded. Accordingly, Base64 encoded attachments must be redacted from MIME e-mails before their production*
- Data layer of document image files (.tiff, .pdf)
- All copied and forwarded counterparts, including :bcc transmittals

### **Production**

Decisions about the medium and format of production, as well as the handling of exceptional attachments, must be made before production of the e-mail can proceed:

- Medium for production: What container will be used for delivery?
  - Electronic transmittal (e-mail attachment, FTP transfer)*
  - External hard drive*
  - Optical disks*
  - Online repository*
  - Hard copies*
- Format of Production: In what form will the data files be delivered?
  - Native (.PST, .NSF)*
  - Discrete files (.eml)*
  - Text files (.txt, .rtf)*
  - Load files (Concordance, Summation)*
  - Image files without data layer (“naked” .tiff)*
  - Image files with data layer (.pdf)*
  - Delimited files*
- Protocol for production of exceptional files, for example:
  - Databases that must be queried to deliver relevant information*
  - Spreadsheets and tables containing Z-axis data and embedded formulae*
  - Voice mail messages and associated metadata*
  - Data requiring proprietary software*
  - Data that could not be opened or decrypted; corrupted data*
  - Other data not lending itself to presentation in a letter size, paper-like format*
  - Scanned data with handwritten entries and marginalia missed by OCR*
- What information will be included in privilege logs?
- What information will be furnished respecting de-duplicated items?

### **Documentation**

Inevitably, something will be overlooked or lost, but sanctions need not follow every failure. Avoid sanctions by documenting diligence at every stage of the discovery effort, to be able to demonstrate why the decision that proved improvident was sound *at the time and place it was made*. Keep a record of where the client looked and what was found, how much time and money was expended and what was sidelined and why.

## Conclusion

Responding to electronic discovery is a complex and challenging task--all the more so as we venture beyond the familiar confines of e-mail to the vast and varied sweep of all digital evidence. In the rush to embrace personal computing, businesses got ahead of sensible records management. Empowering individuals with networked PCs delegated responsibility for evidence preservation without adequate guidance or oversight. In short, businesses—and all of us—reaped the benefits of computers at the cost of discovery becoming harder and more expensive.

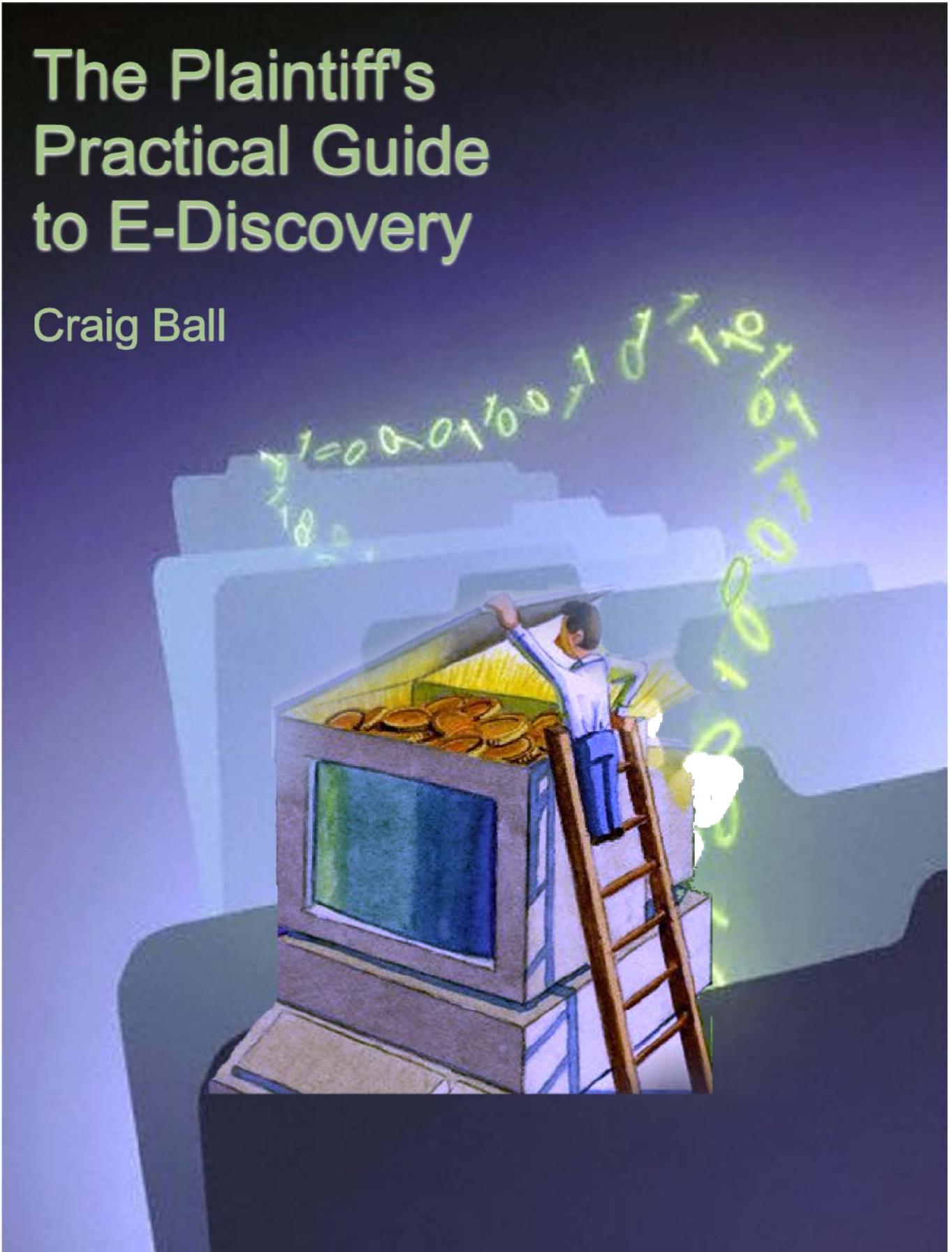
Some argue that we must make it easier and cheaper to litigate by deeming electronic evidence “out of bounds.” Others respond that neither difficulty nor cost can justify curtailing full and fair access to evidence. One fact remains: *most evidence is electronic*. If we want cases decided on the evidence, *discovery means electronic discovery*, and identifying, preserving, harvesting, managing and presenting digital evidence must be as vital and as accepted as cross-examination or trial by jury.

Electronic discovery is discovery in unfamiliar territory. When you figure out the steps and uncover the traps, it’s like any other journey. Here’s hoping this article helps you navigate the e-mail trail.

If you feel this outline omits a step or offers incorrect information, please share proposed additions or corrections with me at [craig@ball.net](mailto:craig@ball.net). For further information about discovery of electronic mail, please read, “Meeting the Challenge: E-Mail in Civil Discovery” (<http://www.ballpoint.org/emailpaper.pdf>).

# The Plaintiff's Practical Guide to E-Discovery

Craig Ball



## The Plaintiff's Practical Guide to E-Discovery, Part I

By Craig Ball

It's challenging. It's expensive. But it's the single greatest litigation advantage for plaintiffs' counsel willing to learn the ropes and aggressively assert their clients' rights. It's electronic data discovery (EDD).

The world has changed, and the traditional approach to discovery--casting the widest net and poring over bankers boxes of documents--is history. Most of the evidence in your case isn't on paper and never will be. The volume of discoverable electronic information is exploding, growing at a rate that makes paper review unthinkable. Although data volume depends on the case--with a car wreck case generating less data than a pharmaceutical products liability class action--even the lowest-end personal computer stores *millions* of pages of information. Hence, volume affects every case.

Getting discoverable data and making sense of it requires plaintiffs' counsel to gain an understanding of where digital evidence lives, the forms it takes and how it's preserved, altered and destroyed. It also entails learning as much as you can about the architecture and operations of the defendant's systems and networks, and how the key players—such as those whose conduct forms the basis of the contemplated claim or suit—interact with a fast-growing universe of digital devices and data repositories.

### Challenges Unique to EDD

Plaintiffs pursuing electronic discovery face entrenched ignorance and outright obstinacy. Evidence on paper was never destroyed and suppressed with the ease and frequency seen with electronic evidence. Folks who wouldn't dream of shredding paper files hit the "delete" button without a moment's hesitation.

One EDD challenge is that foxes guard the henhouse. The common practice in large organizations is to issue a "litigation hold" notice to employees instructing them to retain and segregate relevant electronic evidence. This is the starter pistol for the race by those with something to hide to delete it as quickly as possible. Though motivated to hide workplace pornography or e-Bay shopping, the clumsy delete-o-thons that follow sweep away relevant and discoverable electronic evidence, too.

Another vexing problem is defense counsels' cluelessness about electronic discovery. Your opponent may be a courtroom whiz, but if he or she has a tenuous grasp of computer systems or doesn't understand his or her client's devices and data, defense counsel can't give sound guidance about preserving digital evidence or pose the right questions to knowledgeable IT personnel. It's astounding how often attorneys brag about how *little* they know about computers! Whether due to poor judgment or a client focused on shortsighted cost savings, computer-illiterate counsel don't always seek out the expert help they need. Is this malpractice? Probably, but the lack of expertise is so pervasive, it may take years and several more high-profile e-discovery debacles before lawyers fully appreciate how much their lack of knowledge hurts their clients.

This leaves you on the horns of a dilemma. Do you lay low while evidence is overlooked or lost, banking on spoliation sanctions to protect your client, or do you seek to educate your opponent and improve the odds that you'll get the electronic evidence? The latter is clearly the better

approach, and your ability to succeed in securing sanctions for discovery abuse is only enhanced when you can show how hard you tried to help the defendant “get it.”

### **Failure: The Dirty Little Secret of E-Discovery**

The reality of electronic discovery is that the responding party will fail, partly due to the near-absence of prudent electronic records management. Once upon a time, a discovery request sent a file clerk scurrying to a file room set aside for orderly information storage. There, the clerk sought a labeled drawer or box and the labeled folders within. He didn't search *every* drawer, box or folder, but went only to the place where the company kept items responsive to the request. From cradle to grave, paper had its *place*, tracked by standardized, compulsory practices. Correspondence was dated and its contents or relevance described below the date. Documents and files were sorted and aggregated within a structure that made sense to those who accessed them. A responding party could affirm that discovery was complete on the strength of the fact that they'd looked in the places where responsive items resided. This was the *power of place*, and it freed respondents from the obligation to look elsewhere.

Today, evidence is spread willy-nilly across servers, back up tapes, workstation hard drives, laptops, home systems, personal digital assistants, online storage and thumb drives, so most collection efforts overlook many venues. What records management exists takes a thousand quirky forms as individual employees adopt their own peculiar folder structures and retention practices. Those fearing the consequences of their digital evidence are empowered by the delete key to attempt its destruction. The power of place has waned, making failure inevitable.

Recognizing that your opponents will fail to preserve and produce all discoverable evidence and may even seek to destroy it, what can you do to forestall that failure or ameliorate the harm to your client?

### **Elements of Successful Electronic Discovery**

A successful e-discovery effort entails most or all of the following elements:

- Identifying relevant systems and data
- Compelling preservation of potentially relevant digital evidence
- Seeking production of digital evidence in manageable formats
- Honing preservation and production through “meet and confer” sessions
- Memorializing preservation and production duties as court orders
- Assimilating, analyzing and using the electronic data produced
- Identifying discovery abuses and seeking the Court's intervention

A successful effort also requires us to rethink our traditional approach to discovery. Pursuing paper discovery, we wove expansive nets of the finest mesh to seine anything and everything. Electronic discovery demands the narrow aim of a harpoon. No opponent can satisfy nor court enforce a demand for “any and all electronic communications and records.” That's a fishing expedition. The watchword for e-discovery is, ***Be careful what you wish for lest you get it and have to manage it and pay for its production.***

### **Relevant Systems and Data**

Successful cost-effective electronic discovery is far easier when you know what your case is about and what you need to prove it. Trials still come down to a few key people and documents. You don't win by forcing production of the most data. You win by securing the *right* data.

Start by learning all you can about the defendant's systems. Examine what you have for clues about what else is out there (e.g., by checking path statements on documents or e-mail circulation lists). Check the defendant's website, press releases and public filings for descriptions of IT assets. Talk to former employees about system architecture and data retention practices. Take 30(b)(6) depositions of designated IT personnel—but be sure you also get past the managers and talk to those in the trenches who know about that box of old back up tapes in the storeroom. Get copies of document retention policies and ask witnesses about compliance. Demand that the defendant furnish network topology diagrams and asset tracking inventories for computer hardware, but take these with a grain of salt, as they're often outdated or fail to reflect real-world configurations. Finally, remember that you're not alone. Use resources like the ATLA Exchange to network with other lawyers who've pursued e-discovery against the defendant and to locate qualified electronic discovery and computer forensics experts.

### **Compelling Preservation**

Effective e-discovery begins before suit with your preservation letter to the defendant. The goal of the preservation letter is 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.

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 and marshaled by litigators and in-house counsel who don't understand information systems. *The reality of electronic discovery is that 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.

### **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 is never printed. Preserving electronic data presents its own unique challenges, such as:

- "Touching" data changes it
- Digital evidence is increasingly ill-suited to printing
- All data is simply ones and zeroes which must be interpreted by software to be understood
- 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 by being moved, copied or read. 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.

## 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 can'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.

### **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. For a preservation letter to work, it must be reasonable on its face. Demanding that an opponent retain "any and all electronic communications" is nonsense. If what you want preserved is e-mail or instant messaging or voice mail, *spell it out*.

### **Preservation Essentials**

A preservation letter should seek to halt routine business practices that destroy potential evidence. *As appropriate*, it calls for an end to: server back up tape rotation; electronic data shredding; scheduled destruction of back up media; re-imaging of drives; drive hardware exchanges; sale, gift or destruction of computer systems; and, when 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 your opponent's duty to communicate retention obligations to those with hands-on access to systems.

**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")*.

Focus on specifics—relevant business units, activities, practices, procedures, time intervals, jurisdictions, facilities and key players. Follow the "who, what, when, where and how" credo of good journalism.

The preservation letter is more than just a litany of storage media to be preserved. Its purpose is to *educate* your opponent about the relevant electronic evidence and the importance of taking prompt, affirmative steps to see that evidence remains accessible. Educating the other side isn't a noble undertaking—it's sound strategy. Your goal is to slam the door on the "it was an oversight" excuse.

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. Finally, don't be so focused on electronic evidence that you fail to direct your opponent to retain the old-fashioned paper variety.

### **Nature of the Case**

A pre-suit preservation letter may be your opponent's first inkling they're facing litigation. Don't just assume that the people receiving the preservation letter know what the dispute is about; *tell them*. Furnish sufficient information about the nature of the case to sustain the claim that a reasonable person should have known to preserve particular evidence, and be sure to include names of key players, dates, business units, office locations and events.

### **When to Send**

The conventional wisdom is that preservation letters should be dispatched as soon as potential defendants are identified. Nevertheless, there may be cause to delay sending a preservation letter, as when you face opponents likely to destroy evidence intentionally. A preservation letter could serve as the starting gun and blueprint for their delete-o-thon. In that instance, consider seeking a temporary restraining order or the appointment of a special master. You may elect to wait when your investigation is ongoing and sending the preservation letter will lead to opposing counsel being hired and trigger privileges tied to the anticipation of litigation. There could even be circumstances where you *want* your opponent's routine destruction of information to continue, *e.g.*, when information *unfavorable* to your position will be discarded.

### **Who Gets the Notice?**

If counsel has not appeared for your opponent, to whom should you direct your perfect preservation letter? Here, err on the side of inclusion. Not only the target defendant, but others holding evidence (such as a defendant's spouse, accountant, lawyer, employer, banker, customers and business associates) should be put on notice that you seek preservation.

For corporate defendants, consider preservation letters to the Chief Executive Officer, General Counsel, Director of Information Technologies, Head of Corporate Security and the registered agent for service of process. You're seeking to put all who hold evidence on notice, but you also want broad awareness of the preservation obligation to foster uncertainty in those who might destroy evidence.

Think about who is most likely to *unwittingly* destroy evidence and make sure that person receives a preservation letter. Sending preservation letters to a person likely to destroy evidence *intentionally* is a different story. Here, you may need to balance the desire to give notice against the potential for triggering irretrievable destruction.

## **How *Many* Letters?**

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? Instead of an encyclopedic request, consider drafting your preservation demand as a series of focused requests, broken out by, e.g., type of digital medium, issues, business units, or key players. As an exhibit to a motion to compel or for sanctions, a lean, specific preservation notice beats a bunch of bloated boilerplate.

## **Specifying Form of Preservation**

Preservation letters don't specify the form in which the data should be preserved because you don't want to appear to demand anything more onerous than maintaining evidence in the way it's kept in the ordinary course of business. However, 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***

When should the retention and restoration of server back up tapes be an objective? Though some companies keep selected back up tapes for years, the only legitimate purpose of a back up system is retention of data required to get a business information system "back up" on its feet in the event of disaster. Why would a business need to re-populate its information systems with stale data? Because only the latest data has value, the tapes containing the oldest backed-up information are typically overwritten with newer data. This practice is called "tape rotation," and the interval between use and reuse of tapes is the "rotation cycle."

Data on back up systems would be cumulative of active server data and not a factor in discovery but for the deletion of evidence by users and system maintenance routines. When digital evidence is deleted, back up tape restoration and computer forensics may be the only means to recover missing evidence. Compelling a large organization to interrupt its tape rotation and preserve back up tapes 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 of e-discovery.

A preservation letter should target just the back up tapes likely to contain deleted data relevant to the issues in the case—a feat easier said than done. Additionally, make clear whether you seek back up tape preservation on a going forward basis. For a fixed event, it may be that only the oldest back up set should be pulled from the rotation, whereas for a matter involving continuing injury, ongoing conduct and communications may be relevant and discoverable. Avoid compelling a significantly broader level of tape retention than you can reasonably defend.

### ***Computer Forensics***

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. Information can

be erased from personal computers in only three ways: (1) overwriting the places where the data is stored on disk or tape with new information; (2) encrypting the data and losing the encryption key; or (3) physically destroying the storage media. Otherwise, the data can be restored. Like fingerprints, fibers and DNA left at a crime scene, digital detritus often holds keys to the truth. Computer Forensics is the science dealing with resurrection of deleted data and analysis of digital evidence.

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

For computers (including portable and home systems) used by those named during the period from \_\_\_\_ to \_\_\_\_\_, demand is made that you act to prevent modification, destruction or concealment of evidence on network and local hard drives due to deleting or overwriting files, using data shredding and erasure applications, defragmenting, re-imaging or replacing drives, encryption, compression, steganography or the like. You can preserve data on hard drives by immediate acquisition, authentication and preservation of forensically qualified duplicates (also called a “bitstream images” or “clones”) of all sectors of the drives, as well as recording and preserving the system time and date of each such computer. Forensically qualified images should be labeled to identify date of acquisition, person or entity creating the image and system from which it was obtained. **Be advised that a “back up” is not a forensically qualified method of data preservation and that simply 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 decisive action. Information stored and transmitted electronically must be tracked by the system that stores it and often by the application that created it. Consequently, electronic evidence always exists in at least two parts: the data itself (“the file”) and a separate body or bodies of information describing the data (“the metadata” ).

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. Therefore, 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, copies it or even runs a virus scan, the metadata can be irreparably altered. Most

lawyers don't appreciate that, absent safeguards, simply reviewing electronic evidence can be an act of spoliation.

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 only in the context of Office application metadata—the preservation letter needs to define metadata and educate your opponent about where to find it. The letter should flag common operations that corrupt metadata and perhaps suggest ways by which metadata can be preserved (e.g., by capturing screen shots of detailed folder listings or exporting metadata information to a spreadsheet).

### **The Sharper Tools in the Shed: Meet and Confer**

Proper preservation of electronic data can be costly and complicated. If your opponent is exceptionally well versed in electronic discovery, he or she should seek to meet and confer with you to arrive at an agreed preservation plan. The defendant benefits by reining in the high cost of preservation while minimizing the threat of sanctions. What's in it for your side?

You should welcome a meet and confer opportunity if the defendant furnishes complete and accurate information about the nature and location of their electronic evidence (including back up procedures and retention schemes) and the identity of, and devices used by, key players. Absent such disclosure, it's very risky to agree that the defendant may, e.g., rotate server back up tapes, replace systems or delete older e-mail. Don't concede that the defendant can destroy any information item in any form until the defendant demonstrates that the information lost is not likely to be relevant to any issue in the case or lead to the discovery of admissible evidence. Such representation need to be unambiguously confirmed in writing and supported by a showing that a person with the requisite knowledge and skill actually knows the contents of the media to be overwritten, discarded or destroyed. For voluminous or costly-to-restore data sets, sampling contents is prudent if there is any question as to what information resides on media slated for destruction.

Your agreement may also serve to blunt the defendant's ability to seek cost sharing for the expense of electronic production and open doors to broader or easier access. To gain your client's consent to a narrower preservation obligation, the defendant may be willing to undertake and bear the cost of, e.g., producing digital evidence in your preferred format or computer forensic analysis of key player's office and home computers.

Your opponent isn't the only one who needs to prepare for a meet and confer session. Though it may be difficult early in the case, you must be able to put forward what you want and why you're entitled to it. You don't get the e-mail just because it's there. Be prepared to articulate the relevance and the appropriate interval for the digital evidence you seek.

Finally, it's essential to reduce all preservation and production agreements to writing. Where possible, submit agreed orders to the court, remembering that judges are much more willing to impose sanctions for violations of their orders than for breach of an agreement between counsel.

## **Part II**

Having decided what you need and advised the defendant to preserve it, it's time to seek production. In Part II, we'll look at the pros and cons of production formats and explore common e-mail systems, concluding with tips for getting the most out of your e-discovery efforts and budget.

## The Plaintiff's Practical Guide to E-Discovery, Part II

By Craig Ball

It's challenging. It's expensive. But, it's the single greatest litigation advantage for plaintiffs' counsel willing to learn the ropes and aggressively assert their clients' rights. It's electronic data discovery (EDD). In Part I, we addressed challenges unique to EDD, elements of a successful e-discovery effort and steps to compel preservation of digital evidence. In Part II, we look at the pros and cons of production formats and explore common e-mail systems, concluding with tips for getting the most out of your e-discovery efforts and budget.

### Formats

One of the biggest mistakes a requesting party makes is requesting or accepting production of electronic evidence in a format ill suited to their needs. Electronic evidence can be produced in five principal formats:

- 
- Paper-like image of the data in TIFF or PDF,
- Export of the native data to a common electronic format, e.g., Access database or load file,
- Native data, and
- Hosted data.

Sometimes you'll have the chance to designate the format for production of electronic evidence. Your choice of format should factor in both the type of data being produced as well as the way in which you and your staff are capable of managing the evidence. In a perfect world, you'd want everything in its native electronic format, but in the real world, you may lack the systems and software to deal with and preserve the evidentiary integrity of all native formats. Plus, redaction issues and other fears mean that your opponents will be unwilling to offer native data.

**Paper Production:** I've heard defense counsel deride as "dinosaurs" the plaintiffs' lawyers who ask that electronic evidence be "blown back" to paper. True, converting searchable electronic data to costly and cumbersome paper is usually a step backwards, but not always. Paper still has its place. For example, in a case where the entire production consists of a few hundred e-mails and several thousand e-documents, searching and volume aren't a problem and paper remains about as good a medium as any. But once the volume or complexity increases beyond that which you can easily manage by memory, you're better off insisting on production in electronically-searchable formats.

**Image Production:** Here, production consists of files that are digital "pictures" of the documents, e-mails and other electronic records. These images are typically furnished in accessible file formats like Adobe's Portable Document Format (PDF) or in one of the Tagged Image File Formats (TIFF). As long as the information lends itself to a printed format and is electronically searchable, image formats work reasonably well, but for embedded information (such as the formulae in spreadsheets) or when the evidence moves beyond the confines of printable information (as voice mail, databases or video), image production breaks down. Additionally, the requesting party must insure that the images are accompanied by electronically

searchable data layers and relevant metadata. Beware the defendant who tries to pawn off “naked” TIFF images (devoid of searchable information and metadata) as responsive.

**Exported Formats:** Some electronic evidence easily adapts to any of several production formats. For example, e-mail may be readable in any of several e-mail client programs (Outlook, Eudora, Lotus Notes) or in generic e-mail formats (e.g., .EML). The contents of simple databases can be exported to generic formats (e.g., comma or tab delimited output) and then imported into compatible applications (e.g., Excel spreadsheets to Access databases). When discoverable data lends itself to export formats, you may prefer to obtain exported, delimited data in order to work with it in the compatible application of your choice. The key is to be sure you don't lose any important data, or the ability to manipulate it, in the export/import process. Consider exported data for production of e-mail and simple databases (like contact lists). However, as data structures grow more complex, it's much harder--or impossible--to present exported data in a way that accurately reflects the native environment, forcing you to seek native production.

**Native Production:** In native production, the defendant produces duplicates of the actual data files containing responsive information. The benefit is that, if you have copies of software programs used to create and manipulate the data, you have the ability to see the evidence more-or-less exactly as it appears to the producing party. Sounds great, but native production is not without its problems. The native applications required to view the data in its native format may be prohibitively expensive or difficult to operate without extensive training (e.g., an Oracle or SAP database). Additionally, great care must be taken not to change the native data while viewing it. The rule of thumb is that native production is preferable, but only when you have the experience, expertise and resources to manage native data.

Defendants often resist production of native data because of the great difficulty they face in redacting privileged information. An Outlook post office (.PST) file can hold both discoverable e-mail and privileged attorney-client communications, but as it's a unified and complex database file, it's very difficult to produce the former without also producing the latter. Another risk to defendants is that native data (like Word .DOC files) can contain embedded, revealing metadata.

**Hosted Data:** This is production *without* production, in that the information produced resides on a controlled-access website. The requesting party reviews the data through an online application (similar to a web browser) capable of displaying information from a variety of electronic formats. More commonly, hosted data and online review tools are used by counsel for the producing party to search the production set for privileged and responsive items rather than as a means to afford access to the requesting party. The items identified are then burned to CD or DVD and produced, usually in image formats as discussed above.

### **Rules of Thumb for Formats**

**Word Processed Documents:** In small productions (e.g., less than 5,000 pages), paper and paper-like production formats (.PDF and .TIFF) are fine. As you approach the point where the volume produced creates the need for electronic search capabilities, accept image formats *only* when they include a searchable data layer. Else, demand native production (.DOC, .WPD, .RTF), but be mindful of embedded macros and auto date features that will change the document when opened in its native application. Plus, word processor files can change their appearance and pagination depending upon the printer attached to the computer used to view

the file. Be careful referring to particular pages or paragraphs because the version you see may format differently from the original.

Consider whether system and file metadata are important to the issues in your case. If so, require that original metadata be preserved and a spreadsheet or other log of the original system metadata be produced along with the files.

**E-Mail:** Again, very small productions may be managed using paper or image formats. As volumes grow, accept only electronically searchable formats. These can take the form of individual e-mails exported to a generic e-mail format (.EML files), images files (i.e., .PDF or TIFF) coupled with a text data layer or native production in one of the major e-mail storage formats (.PST for Outlook, .NSF for Lotus Notes, .DBX for Outlook Express). While native formats provide greatest flexibility and the potential to see far more information than a print-like format, don't seek native production if you lack the tools and skill to access the native format without corrupting its contents. All e-mail includes extensive metadata rarely seen by sender or recipient. This header data contains, *inter alia*, information about the routing and timing of the e-mail's transmission. Require preservation and production of e-mail metadata when it may impact issues in the case, particularly where there are questions concerning origin, fabrication or alteration of e-mail. Read on for further discussion of e-mail systems and formats.

**Spreadsheets:** Be cautious about accepting a printout or image file of a spreadsheet. Even if the spreadsheet can be formatted to fit on standard paper without a lot of cutting and pasting, printed spreadsheets lack the very thing that separates a spreadsheet from a table: the formulae beneath each cell. If the spreadsheet is just a convenient way to present tabular data, a print out or image may suffice, but if you need to examine the methodology behind calculations or test different theories by changing variables and assumptions in your opponent's spreadsheets, you'll need native file production. Once again, decide if metadata is important and require its preservation when appropriate. Also, when working with native spreadsheets, be mindful that embedded variables, such as the current date, may update automatically upon opening the file, changing the data you see from that previously seen by others, and metadata about use of the spreadsheet may change each time it is loaded into its native application.

**PowerPoint Presentations:**

If metadata is disclosed, a simple PowerPoint can be effectively produced as an electronically searchable image file in PDF or TIFF but, if a PowerPoint presentation is animated, it's a poor candidate for production as an image because animated images may be omitted or displayed in incomprehensible layers. Instead, native production is appropriate. Like spreadsheets, native production necessitates preservation of original metadata, which may be changed by viewing the presentation.

**Voice Mail:** Voice mail is too often overlooked in electronic productions. A litigant may not be obliged to record phone calls, but once those recordings exist, they should be preserved and are subject to production as any other electronic record. Increasingly, taped phone conversations and messages play a vital role in disputes, such as recordings of broker-client transactions, not to mention all of those companies that claim to record telephone calls "for quality control." There is also an increasing convergence of voice mail and e-mail in businesses, making it more common to see voice mail messages in e-mail boxes. Seek production of voice mail in common sound formats, such as .WAV or .MP3. It's essential that you secure voice mail metadata along with the audio because information about the intended

recipient of the voice message or its time of its receipt is typically not a part of the voice message.

**Instant Messaging:**

Instant messaging or IM is similar to e-mail except that exchanges are in real-time, the client application usually incorporates some way to know if the other party on your list of contacts (“buddy list”) is online and available to chat and messages are only stored at the user’s option. The use of IM in business is growing explosively despite corporate policies discouraging it. Some companies cling to the head-in-the-sand practice of pretending their employees don’t use IM in the workplace and echo that delusion in the replies to discovery. By pretending it doesn’t exist, they naturally take no steps to preserve IM transactions, but in certain regulated environments, notably securities brokerage, the law requires that IM discussions with customers be preserved. Notwithstanding, requests for discovery of IM exchanges continue to be met with the response, “we don’t have any.” Because individual users control whether or not to log IM exchanges, a responding party can make no global assertions respecting the existence of IM threads without checking settings on each user’s local machine. Additionally, even where IM users have not enabled message logging, a computer forensic examination may facilitate recovery of some IM traffic. Although each IM application uses proprietary formats and protocols, most IM traffic is easily converted to plain text and can be produced as an ASCII- or word processor-compatible file.

**Databases:**

Enterprises increasingly rely on complex databases to manage business processes such that the evidence in your case may exist only as a value derived by querying a database. If the database is a rapidly changing one, today’s query may not dislodge data temporally relevant to the matters in controversy, although restoration of back ups or journaled modifications may permit the dataset to be temporarily restored to relevant contents.

Complex databases present enormous discovery challenges. If you seek production of the underlying dataset and application so you can query it directly, you’ll face objections that the request for production of the entire dataset is overbroad and intrudes into trade secrets or the privacy rights of third parties. The producing party may decline to furnish a copy of the database application arguing that to do so would violate its software user license. Further, the cost to license your own copy of complex database software (e.g., Oracle and SAP) and create the hardware environment needed to run it can be prohibitive, even in the largest cases.

If you go this route, specify in your request for production the appropriate back up procedure for the database application geared to capture all of the data libraries, templates and configuration files needed to load and run the database. All publishers of database software publish recommended back up and restore procedures for their products. If you simply request the data without securing a back up of the entire database environment, you may find yourself missing an essential component. By asking that data be backed up according to recommended methodologies, you’ll have an easier time restoring that data, but be sure the method you specify accommodates the output media available to the producing party (i.e., don’t ask for back up to tape if they don’t maintain a tape back up system).

An alternate approach permitting analysis of the underlying data is to request an export of relevant records and fields from the complex database to a common format for import into an off-the-shelf application (e.g., Microsoft Access or Excel). One common export format is the

Comma Separated Variable or CSV file, also called a Comma Delimited File. In a CSV file, each record is a single line and each field in the record is separated by a comma. Not all databases lend themselves to the use of exported records for analysis, and even those that do may oblige you to jump through hoops or engage an expert to get your results admitted at trial.

Although a plain language request for discovery of information contained in an enterprise database should trigger interrogation of the database by the producing party, what if you can't be confident that the query used is suited to the task? In that event, consider formulating specific queries to be run against relevant datasets using the application's own query language and structure. To do so, you will need to understand the application or get expert help. A former employee of the responding party is the ideal candidate for consultation, or you may want to depose a knowledgeable employee of your opponent to learn the ins-and-outs of structuring a query, again assisted by someone who knows the application's query language.

### **Discovery of E-Mail**

Futurist Arthur C. Clarke said, "Any sufficiently advanced technology is indistinguishable from magic." E-mail is one of those magical technologies most of use every day without really understanding how it works. Though a discovery request for "the e-mail" may secure adequate production, understanding e-mail systems helps you to see if something is missing and gauge whether the methods used to assemble responsive e-mail were calculated to locate *all* responsive messages. More to the point, e-discovery is increasingly a two-way street, and plaintiff's counsel needs to prepare for electronic discovery of client e-mail. Can you instruct your client where to find and how to produce e-mail?

*Get the e-mail!* It's the watchword in discovery today. Some label the press for production of electronic mail a feeding frenzy, but it's really just an inevitable recognition of how central to our lives e-mail has become. More than fifty billion e-mails traverse the Internet daily, far more than telephone and postal traffic combined, and the average businessperson sends and receives between 50 and 150 e-mails every business day. At that rate, a company employing 100,000 people could find itself storing *3 billion* e-mails annually. E-mail contributes 500 times greater volume to the Internet than web page content. Trial lawyers go after e-mail because it accounts for the majority of business communications, and e-mail users tend to let their guard down and share things online that they'd never dare put in a memo.

### **Did You Say Billion?**

Aggregate volume is only part of the challenge for discovery and production of e-mail. Unlike paper records, e-mail tends to be natively stored in massive data blobs. The single file containing my Outlook e-mail is over three gigabytes in size and holds some 35,000 messages, many with multiple attachments, covering virtually every aspect of my life, and many other people's lives, too. In thousands of those e-mails, the subject line bears only a passing connection to the contents as "Reply to" threads stray further and further from the original topic. E-mails meander through disparate topics or, by absent-minded clicks of the "Forward" button, lodge in my inbox dragging with them, like toilet paper on a wet shoe, the unsolicited detritus of other people's business. To respond to a discovery request for e-mail on a particular topic, I'd either need to skim/read all 35,000+ messages or I'd have to have a very high degree of confidence that a keyword search would flush out all responsive material. If the request for production implicated material I no longer kept on my current computer, I'd be forced to root around through a motley array of old systems, obsolete disks, outgrown hard drives, ancient back up tapes (for which I have no tape reader) and unlabeled CDs, uncertain whether I've lost

the information or just overlooked it somewhere along the way. The situation isn't much different in corporate America.

### **A Snippet about Protocols**

Computer network specialists are always talking about this "protocol" and that "protocol." Don't let the geek-speak get in the way. An application protocol is a bit of computer code that facilitates communication between applications, i.e., your e-mail client, and a network like the Internet. When you send a snail mail letter, the U.S. Postal Service's "protocol" dictates that you place the contents of your message in an envelope of certain dimensions, seal it, add a defined complement of address information and affix postage to the upper right hand corner of the envelope adjacent to the addressee information. Only then can you transmit the letter through the Postal Service's network of post offices, delivery vehicles and postal carriers. Omit the address, the envelope or the postage--or just fail to drop it in the mail--and Grandma gets no Hallmark this year! Likewise, computer networks rely upon protocols to facilitate the transmission of information. You invoke a protocol—Hyper Text Transfer Protocol—every time you type `http://` at the start of a web page address.

### **E-Mail Systems: POP, IMAP, MAPI and HTTP**

Although Microsoft Exchange Server rules the roost in enterprise e-mail, with Lotus Notes coming in a distant second, these are by no means the most common e-mail system for the individual and small business user. When you access your personal e-mail from your own Internet Service Provider (ISP), chances are your e-mail comes to you from your ISP's e-mail server in one of three ways, POP, IMAP or HTTP, the last commonly called web- or browser-based e-mail. Understanding how these three protocols work—and differ—helps in identifying where e-mail can or cannot be found.

**POP** (for Post Office Protocol) is the oldest and most common of the three approaches and the one most familiar to users of the Outlook Express, Netscape and Eudora e-mail clients. Using POP, you connect to a mail server, download copies of all messages and, unless you have configured your e-mail client to leave copies on the server, the e-mail is deleted on the server and now resides on the hard drive of the computer you used to pick up mail. Leaving copies of your e-mail on the server seems like a great idea, since you have a back up if disaster strikes and can access all your e-mail using different computers. However, few ISPs afford unlimited storage space on their servers for users' e-mail, so mailboxes quickly become "clogged" with old e-mails and the servers start bouncing new messages. As a result, POP e-mail typically resides only on the local hard drive of the computer used to read the mail and on the back up system for the servers which transmitted, transported and delivered the messages. In short, POP is locally-stored e-mail that supports some server storage.

**IMAP** (Internet Mail Access Protocol) is the e-mail protocol used by Lotus Notes and, since 2004, supported by America Online (though AOL continues to furnish a proprietary e-mail client to its subscribers). IMAP differs from POP in that, when you check your e-mail, your e-mail client downloads just the headers (To, From, Date, Subject, etc.) of e-mail it finds on the server and only retrieves the body of a message when you open it for reading. Else, the entire message stays in your account on the server. Unlike POP, where e-mail is searched and organized into folders locally, IMAP e-mail is organized and searched on the server. Consequently, the server (and its back up tapes) retains not only the messages but also the way the user structured those messages for archival. Since IMAP e-mail "lives" on the server, how does a user read and answer it without staying connected all the time? The answer is that

IMAP e-mail clients afford users the ability to synchronize the server files with a local copy of the e-mail and folders. When an IMAP user reconnects to the server, local e-mail stores are updated (synchronized) and messages drafted offline are transmitted. So, to summarize, IMAP is server-stored e-mail, with support for synchronized local storage.

**MAPI** (Messaging Application Programming Interface) is the e-mail protocol at the heart of Microsoft's Exchange Server application. Like IMAP, MAPI e-mail is typically stored on the server, not the client machine. Likewise, the local machine may be configured to synchronize with the server mail stores and keep a copy of mail on the local hard drive, but this is user- and client application-dependent. If the user hasn't taken steps to keep a local copy of e-mail, e-mail is not likely to be found on the local hard drive, except to the extent fragments may turn up through computer forensic examination.

**HTTP** (Hyper Text Transfer Protocol) mail, or web-based/browser-based e-mail, dispenses with the local e-mail client and handles all activities on the server, with users managing their e-mail using their Internet browser to view an interactive web page. Although some browser-based e-mail services support local (POP) synchronization with an e-mail client, typically users do not have any local record of their browser-based e-mail transactions except for messages they've affirmatively saved to disk or portions of e-mail web pages which happen to reside in the browser's cache (e.g., Internet Explorer's Temporary Internet Files folder). Gmail, Hotmail and Yahoo Mail are well-known examples of browser-based e-mail services, although many ISPs (including all the national providers) offer browser-based e-mail access in addition to POP and IMAP connections.

The protocol used to carry e-mail is not especially important in electronic discovery except to the extent that it signals the most likely place where archived e-mail can be found. Companies choose server-based e-mail systems (e.g., IMAP and MAPI) for two principal reasons. First, such systems make it easier to access e-mail from different locations and machines. Second, it's easier to back up e-mail from a central location. Because IMAP and MAPI systems store all e-mail on the server, the back up system used to protect server data can yield a mother lode of server e-mail. Depending upon the back up procedures used, access to archived e-mail can prove a costly and time-consuming task or a relatively easy one. The enormous volume of e-mail residing on back up tapes and the often-high cost to locate and restore that e-mail makes discovery of archived e-mail from back up tapes a big bone of contention between litigants. In fact, most reported cases addressing cost-allocation in e-discovery seem to have been spawned by disputes over e-mail on server back up tapes.

### **Local E-Mail Storage Formats and Locations**

Faced with a discovery request for e-mail, where does one look to find stored e-mail, and what form will that storage take? Because individual e-mails are just text files, they could be stored as discrete text files. However, that's not an efficient or speedy way to manage a large number of messages, so e-mail client software doesn't do it that way. Instead, e-mail clients employ proprietary database files housing e-mail messages, and each of the major e-mail clients uses its own unique format for its database. Some programs encrypt the message stores. Some applications merely display e-mail housed on a remote server and do not store messages locally (or only in fragmentary way). The only way to know with certainty if e-mail is stored on a local hard drive is to look for it. Merely checking the e-mail client's settings is insufficient because settings can be changed. Someone not storing server e-mail today might have been storing it a month ago. Additionally, users may create new identities on their systems, install different client

software, migrate from other hardware or take various actions resulting in a cache of e-mail residing on their systems without their knowledge.

For many, computer use is something of an unfolding adventure. One may have first dipped her toes in the online ocean using browser-based e-mail or an AOL account. Gaining computer-savvy, she may have signed up for broadband access or with a local ISP, downloading e-mail with Netscape Messenger or Microsoft Outlook Express. With growing sophistication, a job change or new technology at work, the user may have migrated to Microsoft Outlook or Lotus Notes as an e-mail client. Each of these steps can orphan a large cache of e-mail, possibly unbeknownst to the user but still fair game for discovery. Accordingly, a producing party shouldn't assert that a user has no e-mail unless the user's local machine(s) and server storage areas have both been thoroughly searched by someone who knows where active and orphaned e-mail reside.

### **Finding E-Mail on Exchange Servers**

150 million people get their e-mail via a Microsoft product called Exchange Server. Though the preceding paragraphs dealt with finding e-mail stores on local hard drives, in disputes involving medium- to large-sized businesses, the e-mail server is likely to be the principal focus of electronic discovery efforts. The server is a productive venue in electronic discovery for many reasons, among them:

- Periodic back up procedures, routine parts of prudent server operation, tend to shield e-mail stores from those who, by error or guile, might delete or falsify data on local hard drives.
- The ability to recover deleted mail from archival server back ups may obviate the need for costly and sometimes fruitless forensic efforts to restore lost messages.
- Data stored on a server is often less prone to tampering by virtue of the additional physical and system security measures typically dedicated to centralized computer facilities as well as the inability of the uninitiated to manipulate data in the more-complex server environment.
- The centralized nature of an e-mail server affords access to many users' e-mail and may lessen the need for access to workstations at multiple business locations or to laptops and home computers.
- Unlike e-mail client applications, which store e-mail in varying formats and folders, e-mail stored on a server can usually be located with ease and adheres to a common file format.
- The server is the crossroads of corporate electronic communications and the most effective chokepoint to grab the biggest "slice" of relevant information in the shortest time, for the least cost.

Of course, the big advantage of focusing discovery efforts on the mail server (i.e., it can deliver up thousands or millions of messages) is also its biggest disadvantage (someone has to extract and review thousands or millions of messages). Absent a carefully-crafted and, ideally, agreed-upon plan for discovery of server e-mail, both requesting and responding parties run the risk of runaway costs, missed data and wasted time.

Server-based e-mail data is generally going to fall into two realms, being online "live" data, which is easily accessible, and offline "archival" data, which may be fairly inaccessible. Absent a change in procedure, "chunks" of data shift from the online to the offline realm on a regular

basis--daily, weekly or monthly—as selected information on the server is duplicated onto back up media and deleted from the server’s hard drives. The most common back up mechanism is a tape drive, really just a specialized version of a cassette tape recorder or VCR. These back up drives store data on magnetic tape cartridges not unlike a VHS tape. As time elapses, the back up media may deteriorate, be discarded or re-used, such that older offline archival data entirely disappears (except, of course, from the many different places it may exist, in bits and pieces, on other servers and local systems).

When e-mail is online, it’s an easy and inexpensive task to duplicate the messages and their attachments in their native form to a discrete file or files and burn those to CD or otherwise transmit the e-mail for review and production. When e-mail is offline, it can be no mean feat to get to it, and the reason why it’s challenging and costly has to do with the way computers are backed up. The customary practice for backing up a server is to make a copy of specified files and folders containing data. Sometimes a back up will copy everything, including the operating system software and the date; but, more often, time and cost constraints mean that only the stuff that can’t be reloaded from other sources gets copied. Another common practice is to only copy all the data every once and a while (e.g., monthly) and just record changes to the data at more frequent intervals.

A daunting challenge to using back up tapes to restore e-mail is the very large volume of duplicate e-mail found on successive back ups. If a user tends to keep e-mail on the server, a back up of the user’s Inbox in one month will look very much like a back up the next. Perhaps 90% of the messages will be identical, month-to-month. Unless steps are taken to filter out these identical e-mails (to “de-duplicate” the data), both the producing party and the requesting party may have to plow through a bloated, redundant production.

Another pitfall of back up tapes is that any e-mail received and deleted between back ups is usually not saved. For example, if the defendant’s e-mail server is backed up nightly, an e-mail received in the morning and immediately deleted likely won’t be backed up because the system no longer “sees” the deleted e-mail in the user’s Inbox.

### **Tips for Seeking E-Mail**

As the volume of e-mail mounts, producing parties are increasingly turning to search tools to identify relevant messages. Be wary of searches based upon subject lines alone. As an e-mail “conversation” threads from one message to the next, aided by the Reply button, contents can veer far afield of the stated subject. Keyword searches alone also tend to overlook a significant percentage of responsive items, particularly when users employ unfamiliar terms-of-art, shorthand references and nicknames in their exchanges. If the producing party employs search tools in lieu of human judgment when responding to discovery, you have a right to know about it and to challenge the methodology if it proves inadequate to the task.

If relevant, be sure to seek production of BCC fields for responsive e-mail, which fields only exist on the sender’s copy of the e-mail. Understand that what a user sees in their e-mail client program (e.g., Outlook or Eudora) is just part of the data that accompanies every e-mail. The data fields seen by the user may be sufficient for your purposes, but sometimes you’ll need more extensive information, such as e-mail header data and routing information.

Don’t give up. There is always at least one “e-mail pack rat” who keeps a copy of everything, notwithstanding policies to the contrary. The more Draconian the policy compelling e-mail

destruction, the greater the likelihood employees have invented ways to circumvent the system (such as by forwarding old e-mail to himself or herself, burning it to disc or shipping it off to a free Gmail account). When opposing counsel says, "There isn't anything else," they may or may not be leveling with you, but they are almost certainly wrong. It's the rare case where a truly exhaustive e-discovery search is even begun prior to the first motion to compel and for sanctions. It's the rarer case where that subsequent search fails to turn up items that should have been produced in the first place.

### **Six Tips for Getting the Most from E-Discovery**

First (and chanting this like a mantra is a good idea), *compel broad e-retention but seek narrow e-production*. This is the approach most likely to be sustained by courts and has the incidental strategic value of being most challenging to your opponent. Narrow requests necessitate careful qualitative review by the producing party.

Second, get your preservation letter and your e-discovery out fast. Data will disappear over time, and you'll be in a poor position to complain about it if you didn't ask for the evidence while it was still around.

Third, don't expect to get it all in a single set of discovery. Digital evidence is everywhere, and you may have to go back to the well many times as you learn more about your opponent's operations and systems. Don't allow the fear of missing something to cause you to cast your net too wide. Keep the focus on what you need to prove your case, and be tenacious.

Fourth, remember that electronic evidence is easy to corrupt but hard to eradicate. It's probably not gone. Few private entities take effective steps to obliterate electronic information, and those that do tend to implement such practices only after the duty to preserve evidence arises. *There is no more compelling evidence than the void left by those who've deleted that which they were obliged to preserve.*

Fifth, get help. You may have to hire an EDD expert to guide you through the first time or two and anytime you're in over your head. Ask the court for help, too. Seek a TRO or protective order and move for appointment of a special master skilled in electronic discovery.

Finally, don't forget: ***what goes around comes around***. Plaintiffs are increasingly vulnerable to e-discovery, so anticipate boomerang discovery, meet and confer early and often, share expectations, seek solutions and don't promise what you may not be able to deliver.

## Twenty Tips for Counsel Seeking Discovery

By Craig Ball

1. Get your preservation letter out early and be *both* specific and general. Assume that the recipients don't know their own systems and don't understand computer forensics. Use the letter to educate them so they can't use ignorance as an excuse.
2. Do your homework: use the Net and ask around to learn about the nature and extent of your opponent's systems and practices. You're probably not the first person to pursue e-discovery against the defendant. Others may know where the bodies are buried.
3. Get your e-discovery out swiftly. Data is going to disappear. You're in a poor position to complain about it if you didn't seek the missing evidence while it was still around.
4. Force broad retention, but pursue narrow discovery.
5. What they must keep and what they must give you are different obligations. Keeping the first broad protects your client's interests and exposes their negligence and perfidy. Keeping requests for production narrow and carefully crafted makes it hard for your opponent to buy delays through objection. Laser-like requests mean that your opponents must search with a spoon instead of a backhoe. Tactically, ten single, surgical requests spread over 20 days are more effective than 20 requests in one.
6. Be aware that opposing counsel may not understand the systems as well as you do, and won't want anyone—especially his client—to know. Help him “get it,” so he can pose the right questions to his client.
7. Question the IT people and focus on the grunts. They've spent less time in the woodshed than the managers, and they know the *real* retention practices.
8. Get their document retention policies, network topology and inventory of computing resources (including laptops, home systems, PDAs and removable media).
9. Invoke the court's injunctive power early to force preservation. The agreement reached to avoid a court order may be better than the relief you'll get from the judge.
10. If you can't get make any headway, seek appointment of a neutral expert or special master.
11. Ask all opponent employee witnesses what they were told to do in the way of e-document retention, then find out what they actually did.
12. Digital data is easily forged. Know how and when to check for authenticity of data produced.
13. Be sure to get metadata whenever it may be relevant.
14. Don't accept image data (TIFF or PDF) when you need native data.
15. Have the principal cases on e-discovery and cost shifting at hand. Tailor your requests to the language of the cases.
16. Set objections for hearing immediately. Require assertions of burden and cost to be supported by evidence.
17. Analyze what you get promptly after you get it, and pin down that it's being tendered as “everything” that's responsive. Follow up with additional requests based upon your analysis.
18. Don't let yourself be railroaded into cost sharing, but if it happens, be sure you're protected from waste and excess by the other side, and leverage your role as underwriter to gain greater access.
19. Be prepared to propose a “claw back” production, if advantageous.
20. Don't accept assertions about cost or complexity unless you know them to be accurate. Independently evaluate all such claims and be prepared to propose alternatives.

# 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.....	36
The Proposed Amendments to the Rules of Civil Procedure.....	36
What is Electronic Evidence Preservation? .....	15
Touching Data Changes It .....	37
Digital Evidence Is Increasingly Ill-Suited to Printing .....	16
Data Must Be Interpreted To Be Used .....	16
Storage Media Are Fragile and Changing.....	16
Digital Storage Media Are Dynamic and Recyclable.....	16
The Duty to Preserve.....	39
Balance and Reasonableness.....	17
Preservation Essentials .....	17
The Nature of the Case .....	18
When to Send a Preservation Letter.....	18
Who Gets the Letter? .....	18
How <i>Many</i> Preservation Letters?.....	19
Specifying Form of Preservation.....	19
Special Cases: Back Up Tapes, Computer Forensics and Metadata .....	19
Back Up Tapes .....	19
Drive Cloning and Imaging.....	43
Metadata.....	45
End Game .....	45

## 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.”<sup>1</sup> 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<sup>2</sup>, but both turn on the subjective awareness of the party failing to

---

<sup>1</sup> 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>)

<sup>2</sup> 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 preserve the information after it knew or should have known the information to be discoverable in the action; and

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.”<sup>3</sup> 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.

### 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

---

(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.”

<sup>3</sup> *Id.* Committee Note to Proposed Rule 37(f), alternative 2.

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 tortious 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<sup>4</sup> 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.

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

---

<sup>4</sup> 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.

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.

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.

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

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.***



**CRAIG BALL**  
**Trial Lawyer & Technologist**  
**Computer Forensic Examiner**

**3402 Cedar Grove**  
**Montgomery, Texas 77356**  
**E-mail: craig@ball.net**  
**Web: cybersleuthing.com**  
**Office: 936-582-5040**  
**Fax: 936-582-4234**  
**Home: 936-448-4321**

Craig Ball is a Board Certified trial lawyer and computer expert with twenty-three years experience resolving a wide range of personal injury and products liability disputes. He's also dedicated his career to teaching lawyers about technology and trial tactics. Craig now limits his work to serving as a court-appointed special master and consultant in computer forensics and to publishing and lecturing on computer forensics, emerging technologies, digital persuasion and electronic discovery. Craig's monthly e-discovery column, "Ball in Your Court," appears in Law Technology News. While Chair of the State Bar of Texas' Technology Advisory Committee, Mr. Ball created the MYTexasBar web portal now used by over 45,000 Texas lawyers. Named as one of the Best Lawyers in America and a Texas Superlawyer, Craig is a recipient of the Presidents' Award, the State Bar of Texas' most esteemed recognition of service to the profession.

#### **EDUCATION**

Rice University (B.A., triple major, English, Managerial Studies, Political Science, 1979); University of Texas (J.D., with honors, 1982); Oregon State University (Computer Forensics certification, 2003); EnCase Intermediate Reporting and Analysis Course (Guidance Software 2004); WinHex Forensics Certification Course (X-Ways Software Technology AG 2005).

#### **SELECTED PROFESSIONAL ACTIVITIES**

Law Offices of Craig D. Ball, P.C.; Licensed in Texas since 1982.

Board Certified in Personal Injury Trial Law by the Texas Board of Legal Specialization

Certified Computer Forensic Examiner, Oregon State University and NTI

Admitted to practice U.S. Court of Appeals, Fifth Circuit; U.S.D.C., Southern, Northern and Western Districts of Texas.

Member, Editorial Advisory Board, Law Technology News (American Lawyer Media)

Special Master, Electronic Discovery, Federal and Harris County (Texas) District Courts

Instructor in Computer Forensics, United States Department of Justice

Special Prosecutor, Texas Commission for Lawyer Discipline, 1995-96

Council Member, Computer and Technology Section of the State Bar of Texas, 2003-

Chairman: Technology Advisory Committee, State Bar of Texas, 2000-02

President, Houston Trial Lawyers Association (2000-01); President, Houston Trial Lawyers Foundation (2001-02)

Director, Texas Trial Lawyers Association (1995-2003); Chairman, Technology Task Force (1995-97)

Member, High Technology Crime Investigation Association and International Information Systems Forensics Association

Member, Texas State Bar College

Member, Continuing Legal Education Comm., 2000-04, Civil Pattern Jury Charge Comm., 1983-94, State Bar of Texas

Life Fellow, Texas and Houston Bar Foundations

CLE Course Director: E-Discovery A to Z (NY, Chicago, SF, Boston, Washington, D.C. and Minneapolis) 2004;

Electronic Evidence and Discovery 2004, 2005; Advanced Evidence and Discovery Course 2003; 2002;

Enron—The Legal Issues, 2002; Internet and Computers for Lawyers, 2001-02; Advanced Personal Injury Law

Course, 1999, 2000; Preparing, Trying and Settling Auto Collision Cases, 1998.

Member, SBOT President's "Vision Council" on Technology, 1999-2000; Strategic Planning Committee Liaison,

2001-02; Corporate Counsel Task Force 2001-02

#### **ACADEMIC APPOINTMENTS AND HONORS**

The March 2002 CLE program planned by Mr. Ball and Richard Orsinger entitled, "Enron—The Legal Issues" received the Best CLE of 2002 award from the Association for Legal Education

National Planning Committee, Legal Works 2004 (San Francisco)

Recipient, State Bar of Texas Presidents' Award (bar's highest honor), 2001

Faculty, Texas College of Trial Advocacy, 1992 and 1993  
Adjunct Professor, South Texas College of Law, 1983-88  
Listed in "Best Lawyers in America" and Selected as a "Texas Super Lawyer," 2003 and 2004  
Rated AV by Martindale-Hubbell

**LAW RELATED PUBLICATIONS AND PRESENTATIONS**

Craig Ball is a prolific contributor to continuing legal and professional education programs throughout the United States., having delivered over 350 presentations and papers. Craig's articles on forensic technology and electronic discovery frequently appear in the national media, including in American Bar Association, ATLA and American Lawyer Media print and online publications. He also writes a monthly column on computer forensics and e-discovery for Law Technology News called "Ball in your Court." The presentation, "Craig Ball on PowerPoint," is consistently the top rated educational program at the ABA TechShow.