

In This Issue...

Federal Practice

ESI Preservation and Collection – Issues and Solutions
Article Contributed by Pierre Grosdidier, Haynes and Boone, LLP..... 1

Alternative Dispute Resolution

Former Employee's Case Dismissed on Motion to Stay Pending Arbitration..... 9
Motion to Compel Arbitration of CitiFinancial Employment Dispute Granted Absent "Compelling Evidence" of Waiver 10

Class Actions

Judge Posner Rules Plaintiff of "Flopped" Class Entitled to Only \$17,000 in Fees..... 11
Fourth Circuit Rules – Again – for Cancer Patients in Supplemental Health Insurance Case 12

Constitution Law

Fifth Circuit Holds Junked-Vehicle Ordinance Does Not Violate First Amendment 13
Sixth Circuit Holds Plaintiff Did Not Have a Protectable Property Interest in a City Pool Token, But Possessed a Clearly Established Constitutionally-Protected Liberty Interest Not to be Banned from City Recreational Property Without Procedural Due Process 15

Damages & Remedies

New York District Court Reduces Attorneys' Fees Award Due to Number of Hours Attributable to Supervising and Training of Lead Attorney 17
Ninth Circuit Affirms Dismissal of Declaratory Judgment Action for Lack of Subject Matter Jurisdiction Where Plaintiff Had No Private Right of Action to Enforce Provisions of Federal Communications Act..... 17

Federal Appellate Procedure

Eleventh Circuit Determines It Has Jurisdiction to Hear Appeal Solely On Grounds of Qualified Immunity..... 19

Federal Civil Procedure

Virginia District Court Holds that Parties to a Mandatory Forum Selection Clause May Not Consent to Removal..... 20
Eighth Circuit Affirms Summary Judgment in Defendants' Favor, Declining to Toll Statute of Limitations Where Plaintiff Could Not Establish Fraudulent Concealment 21
Fifth Circuit Affirms Denial of Motion for Continuance that Served as Death Knell for *Pro Se* Plaintiff's Discrimination Suit Against U.S. Postal Service 22

Federal Evidence

New York Court Excludes Consumer Survey in Disney Trademark Litigation 23
Tenth Circuit Finds Co-Conspirator Hearsay Statements Were Not Erroneously Admitted into Evidence Because No Showing was Made that the Statements Were Hearsay 24

Litigation News

Bloomberg News Daily Litigation Wrap Up 25

Bloomberg Law

Bloomberg Continuing Legal Education 28

Federal Practice

ESI Preservation and Collection – Issues and Solutions

Article Contributed by: Pierre Grosdidier, Haynes and Boone, LLP

Introduction: Scope and Purpose of this Article

E-discovery is complex, expensive and daunting for attorneys who are not computer savvy. It is also a potential minefield. In *Qualcomm Inc. v. Broadcom Corp.*, the court ruled that Qualcomm's lawyers "chose not to look" in the right places for the right documents in what it called a "monumental discovery violation" involving 46,000 e-mails.¹ The court imposed an \$8.6 million [Rule 37](#) sanction against Qualcomm, and referred six of its outside counsels to the state bar for possible disciplinary proceedings.² How do 46,000 e-mails elude attention? Whatever the reason, the best way for counsel to avoid a similar disaster is to fully understand the client's computer systems and to directly manage the preservation and collection of electronically stored information (ESI). Counsel must be able to personally and confidently determine whether all sources of ESI have been identified and explored. Knowledge of e-discovery law is not enough to achieve this goal. Counsel needs to understand computer systems and expect to manage the preservation and collection of ESI from scores of custodians and, possibly, hundreds of computers.

The purpose of this article is to describe the basic issues that attorneys face when tasked with preserving and collecting their client's ESI for litigation and to offer tangible and practical solutions.³

ESI Preservation and Collection: What to Avoid

The best-avoided way to preserve ESI is to first argue with opposing counsel what the scope of the preservation should be and then to try to proceed with the actual collection. By the time counsel resolves to collect the ESI, it is likely that some is irretrievably lost. At best, some employees will have neglected to read the litigation hold memo or will have misunderstood its directives. Worse, a rogue employee might intentionally delete compromising ESI.

In *G.K. Las Vegas Ltd. P'ship v. Simon Prop. Group*, the parties negotiated for several months over the scope of e-discovery.⁴ Plaintiffs' claims were in the hundreds of millions of dollars.⁵ The parties negotiated the relevant time frame for which documents would be collected, the search terms that would be used to

identify relevant documents, and the computers (servers and personal computers) and databases that would be searched.⁶ The parties also identified five present or former principal “employees/custodians” of the plaintiffs who may have sent or received relevant e-mails or documents.⁷ These principal custodians’ office computers were to be subjected to electronic searches for documents responsive to the search terms.⁸

Almost a year after discovery began, defendants learned that the five principal custodians had not preserved e-mails and other ESI on their personal office computers, and that these computers had not been searched.⁹ Plaintiffs’ counsel argued that the searches were, at this point, unnecessary, given that there was no longer reason to believe that the computers contained relevant ESI.¹⁰ Nonetheless, plaintiffs’ counsel offered to image the computers and perform the searches at the cost of some \$20,000, to be borne by the defendants.¹¹ The court rejected plaintiffs’ arguments and ordered the searches performed at their expense.¹²

The take-away from this case is that plaintiffs procrastinated over a \$20,000 expense and exposed themselves to possible accusations of spoliation when their multi-hundred million dollar claims were at stake. Rather than wait for the parties to agree on the scope of e-discovery, plaintiffs’ counsel should have preemptively ordered the custodians’ computers imaged as soon as litigation was foreseeable in order to ensure the preservation of their ESI.

ESI loss through negligence or oversight is not counsel’s only worry. In some cases, ESI may literally have to be taken away from the client to remove any possibility of spoliation.¹³ In *In re Hawaiian Airlines, Inc.*, plaintiff, Hawaiian Airlines, accused defendant, Mesa Air Group, of having improperly retained and used confidential information that had been made available under narrow terms to bona fide potential investors, including Mesa.¹⁴ A Mesa attorney issued a litigation hold memorandum the day after Hawaiian filed its complaint.¹⁵ Evidence eventually established that one of Mesa’s senior executives used a “disk wiping” program to intentionally wipe the hard drives of his two business laptops months after the lawsuit was filed.¹⁶ Additional evidence showed that the executive deleted files from his personal shared drive.¹⁷ The shared drive files were partly recovered through back-ups but not so the laptop files, which were permanently lost.¹⁸

In addition to imposing sanctions, the judge castigated Mesa for its failure to take reasonable steps to prevent the destruction of evidence.¹⁹ The judge stated that issuing the preservation memorandum was not enough, and that Mesa should have made back-ups of the shared drive and the laptops “promptly” after the lawsuit was filed.²⁰ These back-ups would have been neither costly nor burdensome.²¹ In the judge’s words, “Mesa could and should have taken reasonable steps to prevent all of its employees from doing wrongful and foolish things, like destroying evidence, under the pressure of litigation.”²² Even though the evidence indicated that the executive acted alone, Mesa “facilitated [the executive’s] misconduct.”²³

In any lawsuit where ESI is involved, the prudent attorney should counsel her client to issue the litigation hold and preemptively collect all relevant ESI from all the client’s custodians.

Identifying the Custodians

A custodian is formally defined as a “[p]erson having control of a network, computer or specific electronic files.”²⁴ In the context of ESI preservation and collection at the onset of a lawsuit, the term custodian is more narrowly used to designate a person who is knowledgeable with the facts of the case and whose ESI is therefore likely to be relevant to the lawsuit. Every custodian must be placed on notice of the litigation hold, and his (or her) ESI should be preserved as soon as possible.

The case law is relatively silent on who qualifies as a custodian. The court in *Zubulake v. UBS Warburg LLC* (“*Zubulake IV*”), the seminal case on e-discovery, stated that the preservation obligation extended to the “key players” in the litigation, *i.e.*, “those employees likely to have relevant information . . . in the case.”²⁵ However, that definition is not free of ambiguity because who is “likely to have relevant information” is arguably unclear at the start of the lawsuit when the preservation obligation is triggered but relatively little is known about the lawsuit and its actors. *Zubulake*’s definition of a custodian could also lead to confusion because many employees can have relevant information about a lawsuit without being “key players,” as that term is commonly understood, in the events that led to the lawsuit. An administrative assistant, for example, is rarely construed as a “key player” in the everyday sense of the word, but her computer can prove to be a rich source of relevant ESI.

One approach is to agree with opposing counsel on who are the custodians. The danger with this method, as *Simon Prop. Group* demonstrates, is that months can pass before the parties agree on the lists of names.²⁶ The second difficulty is that it is easy to overlook someone in the initial list, and that person’s ESI may be lost by the time counsel recognizes the oversight.

Even though it is certainly necessary to discuss the custodian lists with the opposing side early in the case, the more conservative approach is for counsel to independently draw up a list of his client’s custodians, erring on the side of over-inclusiveness. The list of custodians should include any and all persons who have any connection whatsoever to the subject matter of the lawsuit.²⁷ The point in creating an over-inclusive list of custodian is not that all their ESI must be produced to opposing counsel during discovery but that the ESI will have been preserved in the event that it needs to be produced.

Counsel can develop the list of custodians on the basis of the facts of the case, interviews with known “key players” and some sleuthing. E-mail distribution lists regarding subject matters that are relevant to the lawsuit can help identify custodians. Administrative assistants of custodians (both past and present) should also be designated as custodians.

Executive administrative assistants will sometimes be better sources of ESI than the executives themselves, as the latter may shun computers and request that all e-mail traffic proceed through their assistants. Many assistants also keep everything as a matter of habit, and their computers can be troves of ESI. The same is true of project administrators.²⁸ Former employees should also be designated as custodians if they took responsive ESI with them when they left (for example when they are allowed to leave with their laptop) or if they continue to work as contractors with a company laptop or with their own.²⁹

Issuing the Litigation Hold

Once a party is on notice of potential or pending litigation, the “obligation to preserve evidence runs first to counsel.”³⁰ Counsel needs to act proactively to ensure that all ESI is preserved. In practice, counsel should quickly issue a litigation hold memorandum and meet with the custodians and the client’s information technology (IT) team to ensure that they all understand their preservation obligations.

At a minimum, the litigation hold memorandum should include:

- a.) A description of the subject matter of the documents that must be preserved. For example, if the lawsuit is about the collapse of a bridge, then the preservation obligation applies to all documents that deal with the bridge from the earliest stage of conception to the accident and beyond. Counsel should strive to describe the documents that are relevant to the claims (and counter-claims) of the lawsuit in terms that employees of the client will understand, making allowance for the possibility that new claims may be added in the future. Relevant documents are more likely to be preserved if the employees know and understand what the lawyers want to preserve.
- b.) A description of the devices and media that are covered by the litigation hold, such as computers (including home computers), hand-held devices, CDs and DVDs, thumb drives, etc. Counsel should think broadly about the possibilities.
- c.) A description of the types of documents that are covered by the litigation hold, such as e-mails, word-processed documents, spreadsheets, design files, presentations, drafts and final versions, voice mails, text messages, etc.
- d.) Whether the preservation obligation runs forward in time. In disputes where, for example, damage mitigation is an issue, the obligation to preserve applies to future, as well as to past documents. The conservative approach is to preserve relevant documents on a going-forward basis.

The litigation hold memorandum should also contain a clear explanation of how custodians are to preserve documents on a day-to-day basis:

- a.) Relevant e-mails must be saved, not deleted. Clearly non-relevant e-mails can be deleted, but should not be purged from the recycle bin (or the delete folder) for several days, or at least time enough to allow the e-mail server’s back-up program to save them (back-up programs typically run nightly).
- b.) Work-related e-mails in personal e-mail accounts, such as Yahoo!, AOL, etc., must be preserved, and auto-delete functions in these accounts, if any, must be immediately disabled. Counsel should quickly inquire whether the owners of these accounts control the auto-delete function. If they do not, measures must be taken to preserve the relevant contents of the accounts.
- c.) Relevant electronic files must be retained and must not be modified. If a file must be edited, it should first be copied and saved as a new version, and all successive versions should be preserved. A good rule of thumb is that files that are edited frequently, e.g., project status or project tracking files, should be saved as new versions daily or each time the files are distributed to others.
- d.) Relevant electronic files that are saved on a server must be saved in designated shared drives to avoid file dispersion.³¹ File dispersion increases the number of server folders that must be preserved, which increases preservation complexity and cost.

Drafting and distributing the litigation hold memorandum, and discussing it with the custodians is still not enough. Counsel must act proactively to preserve the ESI. *The obligation to preserve runs to counsel.*³² Consequently, counsel should not rely on the client (business people) to turn in their ESI. Counsel must personally organize and supervise the collection of all the custodians’ ESI.

In *Cache la Poudre Feeds, LLC v. Land O’Lakes, Inc.*, Land O’Lakes was sued for trademark infringement and unfair competition.³³ Land O’Lakes’ in-house counsel issued a litigation hold, but relied on employees to locate and surrender documents “related to the litigation.”³⁴ Counsel did not independently verify the completeness of employees’ production and made no attempt to stop the practice of “wiping clean” the disks of departing employees.³⁵ In deposition, counsel revealed his limited understanding of Land O’Lakes’ computer systems and ESI back-up procedures.³⁶ The court chastised counsel for failing to meet the standards of [Fed. R. Civ. P. 26](#) though 37.³⁷ The court stressed that counsel had an affirmative duty

to follow-up after issuing the litigation hold.³⁸ “A ‘litigation hold,’ without more, will not suffice to satisfy the ‘reasonable inquiry’ requirement in [Rule 26\(g\)\(2\)](#).”³⁹ To follow through with a litigation hold and collect all the custodian’s ESI, counsel needs to meet with the IT group and understand the systems under their responsibility.

Meeting with the IT Group

Counsel should meet with the client’s IT group to ensure that the litigation hold memorandum is not lost on its audience. The meeting(s) objectives are: (1) to ensure that communication channels are established between counsel and the highest level in the IT hierarchy; (2) to understand the client’s IT systems, including its standard back-up procedures; (3) to ensure that IT implements its own ESI preservation measures; and (4) to ensure that the custodians have the means necessary to preserve their ESI.

Counsel Should Establish Proper Communication Channels at the Highest Level in the Client’s IT Hierarchy

Counsel should meet with individuals at the highest level of the IT hierarchy in order to be accurately briefed on the client’s IT systems, and in order to ensure that the decision makers in the IT group know first-hand about all the ESI preservation obligations and issues. Never underestimate the importance of speaking to the right person in IT.

In *GTFM, Inc. v. Wal-Mart Stores, Inc.*, the court admonished Wal-Mart’s in-house counsel for failing to review the company’s computer capabilities with a vice-president in Wal-Mart’s MIS department.⁴⁰ The plaintiff had requested, in December 1998, all sales records since January 1, 1997.⁴¹ Wal-Mart’s counsel responded, and later insisted in court, that records older than five weeks were not available from Wal-Mart’s computer systems.⁴² A year later, in December 1999, plaintiff took the deposition of a Wal-Mart MIS vice-president, who revealed that Wal-Mart’s computers retained sales records for more than a year.⁴³ Therefore, by December 1998, Wal-Mart should have been able to produce sales records going back to December 1997.⁴⁴ However, by the time of the MIS vice-president’s deposition, the 1998 records were no longer available.⁴⁵ The court stated that Wal-Mart’s counsel’s inquiries about its client’s computer systems were “certainly deficient.”⁴⁶ Counsel should have “obvious[ly]” reviewed Wal-Mart’s computer system capabilities with the MIS vice-president.⁴⁷ The court sanctioned Wal-Mart by granting plaintiff attorneys’ fees and access to Wal-Mart’s computer records and facilities.⁴⁸

As a result of the meetings, the IT executive should clearly understand the importance of the ESI preservation effort, commit to assign adequate resources to support the effort, and leave open a direct channel of communication between counsel and the executive.

Counsel Must Understand the Client’s IT systems

At least one federal district imposes on counsel a duty “to become knowledgeable about their client’s information management system.”⁴⁹ The *Zubulake V* court went even further, holding that “it is necessary to *thoroughly* understand the responding party’s computer system, both with respect to active and stored data.”⁵⁰ Therefore, counsel should not be content to just know how frequently IT rotates its back-up tapes. Counsel should understand the client’s network topology, how incoming, outgoing, and internal e-mail traffic is managed, how ESI is saved in servers, how ESI is backed-up, etc. A comprehensive understanding of the IT system may require more than one meeting, especially if the client’s operations are spread over several locations. Counsel should budget ample time (and travel funds, if necessary) for this inquiry. All findings should be documented in a comprehensive memorandum.

In some cases, a key threshold issue will be to identify what are the relevant IT systems. Most civil disputes are about who wrote what and when, as evidenced in e-mails and their attached files. Some disputes are about what happened *inside* a sophisticated computer system, such as a real-time trading system, a real-time operating system for a processing plant or an Internet web site.⁵¹ ESI is everywhere nowadays: in security cameras, in GPS-connected tracking devices, in hand-held devices, on Internet pages. Counsel should try to think imaginatively about where ESI relevant to the lawsuit is, or might be located, and act proactively to ensure its preservation. At the start of every lawsuit that involves ESI, counsel should identify all the relevant IT systems in the underlying dispute and take measures to become familiar with all of them.

IT Must Implement Its own ESI Preservation Measures

It is not sufficient to ensure that custodians preserve their ESI. IT must do so as well. The overall goal of IT’s ESI preservation measures must be to preserve what ESI exists at the time the litigation hold is issued and to preserve relevant ESI on a going-forward basis. Some measures are straightforward. For example, a necessary first step is to ensure that all e-mail auto-delete functions are disabled.⁵²

Another simple step is to stop the recycling of former employees’ computers. Most IT groups “reformat” the hard drive of departed employees’ computers before passing them on to other employees. That procedure can continue *only if* IT first images the hard drives to preserve their contents. A better procedure is to remove the hard drive for preservation, and to swap a new one into the computer.

Counsel might consider requesting IT to enable the journaling function in the e-mail server, if that function is not already activated. The journaling function preserves a record of all e-mails sent and received by the e-mail server, separately from the users’ e-mail folders.

Counsel may have to act quickly to preserve ESI contained in real-time systems, as these systems can have notoriously short data retention cycles. It is also good practice to inquire with the client's Human Resources (HR) department whether layoffs are anticipated as a result of the lawsuit (or any other reason). Counsel should discuss with IT and HR whether special measures are required to protect the ESI of the persons expected to be released.

Back-Up Tapes

The more substantive problems concern what to do about the back-up tapes. The Sedona Principles and the case law state that, in general, there is no need to interrupt the recycling of back-up tapes.⁵³ *Zubulake IV* agrees with The Sedona Principles but distinguishes between "accessible" and "inaccessible" back-up tapes.⁵⁴ Accessible back-up tapes are those that are "actively used for information retrieval," whereas inaccessible back-up tapes are "those typically maintained solely for the purpose of disaster recovery."⁵⁵ This distinction is also not without ambiguity. Few tapes, nowadays, are made for "active information retrieval," and most data that require frequent access are kept on disk.

Perhaps a distinction can be made between back-up tapes that are maintained for disaster recovery and back-up tapes that are maintained for regulatory reasons. The first store all data from designated file folders, whereas the other only store data from specific applications, e.g., data from a trading system.⁵⁶ In either case, data would be encrypted or compressed on both categories of tapes, and it is not clear that one would be more accessible than the other or that back-up tapes made for regulatory reasons would ever be recycled.

In any event, there are two reasons to proceed very cautiously with disaster recovery back-up tapes. The first is that the tapes may be the only source of relevant ESI if custodians accidentally delete files or are tempted to purge them upon hearing of the lawsuit. In *In re Hawaiian Airlines*, server files that were deleted by a rogue executive were recovered through the back-up tapes.⁵⁷ When careless or rogue employees delete ESI, the ESI may be found only on the back-up tapes and will be lost forever unless their recycling is stopped.

Zubulake IV recognizes this possibility and, accordingly, qualifies its "general rule" that back-up tapes may continue to be recycled.⁵⁸ Back-up tapes must be preserved if they contain ESI that is "not otherwise available."⁵⁹ This qualifier essentially negates the general rule because it is impossible to know at the start of a lawsuit whether (or not) back-up tapes are the only source of some ESI.

The second reason to stop the recycling is that the technology has changed (as it always does) since the *Zubulake* rulings were issued. Back-up tapes are increasingly replaced by back-up save-sets on disks, which are easier to manipulate than tapes. Perhaps more importantly, search and mining techniques of compressed save-sets have so improved that

the cost "barrier" to exploiting them has lowered considerably. Therefore the "burden or cost" argument in [Fed. R. Civ. P. 26\(b\)\(2\)\(B\)](#) may become harder to make in the future for save-sets on disks.⁶⁰

Since no two IT systems are exactly the same, there is no universal list of preservation measures IT should adopt. However, the methodology that counsel should follow is nearly always the same. Specifically, counsel must identify what ESI needs to be preserved and work with IT to develop appropriate measures to safeguard the ESI.

Typically, daily back-ups are done to disk and not to tape because disks are more reliable and increasingly affordable.⁶¹ Full back-ups are performed weekly, usually on weekends and are supplemented with daily incremental back-ups.⁶² The disk is sized to keep about six months of back-ups on-line, and the oldest save-sets are overwritten by the newer ones. Once a month, a full back-up is archived to tape, which is then placed in storage.⁶³

For such an installation, counsel must first ensure that the archival tapes are preserved, even if they are not being recycled. Counsel should also ensure that the weekly full back-ups on disk are preserved, as well as the daily incremental back-ups. If disk space is an issue, the back-up save-sets can be moved to tapes. The daily incremental back-ups should be preserved because they contain ESI that may not exist in the weekly backups. The weekly back-ups are snapshots of a server on two successive Saturday nights. Files that are created at the start of the week and deleted before its end will be included in one or more of the daily incremental back-ups, but not in the weekly back-ups.⁶⁴

On a going-forward basis, counsel could recommend that IT perform two sets of back-ups. One set of back-ups could be the continuation of the old back-ups and cover the entire system. That set of back-ups can continue on a new rotation basis. The other back-ups would collect only the custodians' ESI, and would be preserved indefinitely.⁶⁵

All preservation measures should be documented in a comprehensive memorandum to file. This memorandum will be invaluable to answer detailed preservation questions that will arise months, if not years, later.

Custodians Need the Means Necessary to Preserve Their ESI

Storage space is the issue most frequently raised by custodians after receiving notice of the litigation hold. Custodians frequently run out of space on their computers, on their e-mail folders and sometimes on their shared drives. IT can also run out of space as the custodians invariably turn to IT and request greater disk space allocation quotas.

Counsel should quickly place the IT group on notice that disk space will likely be a limitation, and that steps should be

taken immediately to forestall this problem. At the same time, counsel should place the client's controller on notice that IT might want to order a large disk array within a week or two, and that the purchase should be expedited.⁶⁶

Space limitations for e-mails and for shared drives can be resolved relatively easily through the purchase of large disk arrays. With plenty of space on the servers, IT can simply increase the amount of disk space allocated to each custodian. Storage space limitations on custodians' personal computers are no so easily solved. Should a custodian run out of space on her computer, the proper solution is to replace the computer's hard drive. The old hard drive must be preserved, and its image can be copied onto the new hard drive. The custodian will welcome the swap, despite the temporary inconvenience, if it gives her a larger hard drive.

Do not allow custodians who run out of space on their personal computers to get an external hard drive. The custodians will inevitably move some of the files on their computers to the hard drive. The move will modify the files' metadata, and possibly destroy relevant evidence. As described above, the better solution is to swap the hard drive for a bigger one.

Collecting the ESI for Preservation

Counsel should not rely on the client's IT group to perform the ESI collection. Although this solution might be appropriate in some cases, the better decision is to hire a third-party consultant with recognized computer forensic expertise. First, the client's IT group is likely to be already at capacity dealing with day-to-day issues, and will not have the resources to staff the ESI collection.⁶⁷ The second reason is that the client's IT group is generally adequate – only if everything goes well. As soon as difficulties arise, such as issues with tampered computers, or hard drives that are defective but recoverable, computer forensic expertise will be required that the IT group will lack. A third-party consultant will also be required if non-party (to the lawsuit) computers must be imaged. Beyond the obvious custody transfer issues that arise if the client's IT group does the imaging, the non-party will probably accept no-one near its computers other than a neutral and expert third-party consultant.

ESI should be collected by making forensic copies (colloquially known as images) of the original media. Forensic copies preserve everything on the media, "including all active and residual data and unallocated or slack space on the media."⁶⁸ Simple file copying preserves only active files and not the "structure" of the ESI on the media. Only an image of a custodian's computer hard drive can preserve evidence of tampering with files, including attempts to wipe the hard drive.⁶⁹

Counsel should investigate where relevant ESI is located and direct the consultant to image everything so identified.

At a minimum, forensic copies should be made of the following sources of ESI:

- a.) The custodians' work computers. Each custodian's work computer must be imaged. In some cases, it will make more sense to "swap" the hard drive, i.e., to keep the original hard drive, and to insert a new hard drive in the computer that is an image of the original.
- b.) The custodians' home computers. Personal home computers should also be imaged if custodians keep work files on them. The better practice is to image the entire hard drive to preserve evidence that the custodians purged files.
- c.) The custodians' peripheral devices. All the custodians' CDs, DVDs, "thumb" or USB drives, cell phones (for text messages), hand-held devices, e.g. BlackBerrys' or iPhones.
- d.) The custodians' "personal shared drives." Employees are usually assigned file folders on company servers where they can save files other than on their own computers. These file folders are typically called personal shared drives and must be forensically captured.
- e.) The custodians' "group shared drives." IT groups also provide employees with file folders that are dedicated to projects. These folders are not assigned to specific employees, but to specific projects. The folders that belong to the project that is the subject of the lawsuit must be forensically captured.⁷⁰
- f.) "Misplaced" files can be located by running a keyword search over the entire server. If relevant files are located in folders other than the relevant personal and group share drives, these entire folders should be forensically captured (not just the files).
- g.) All relevant files in Document Management Systems. These files can be identified by project number or custodian name.
- h.) The custodians' native e-mail folders. The native e-mail folders are those that reside on the custodian's computer. Normally, these folders are copied when the computer is imaged.
- i.) The custodians' server-based e-mail folders. These folders reside on the e-mail server.
- j.) The custodians' other e-mail files. Counsel should ask whether custodians have saved e-mails in save-sets such as, for example, Outlook .PST

files. Counsel should make sure that these files are captured as part of the ESI collection work.

- k.) The custodians' personal e-mail account(s) for those custodians that send or receive work e-mails on their personal account(s).⁷¹
- l.) Last, but perhaps most importantly, the e-mail server's journals should be copied. The journals normally contain all e-mails that are received or sent by the e-mail server. For this reason alone, the journals are a treasure trove of ESI. If the journaling function of an e-mail server is enabled, and the journals are saved, all e-mails that went through the server are technically recoverable, even those that were deleted by the senders or recipients.⁷²

The above sources of ESI should only be treated as the obvious list of places where to look, but *Zubulake V* requires counsel and its client to look for *sources* of ESI.⁷³ ESI is ubiquitous and counsel should ask questions and exercise her imagination to locate non-obvious sources of ESI.

Discarded or "recycled" computers or hard drives should never be overlooked. Most often, it may simply be a matter of collecting and analyzing an old hard drive gathering dust in a custodian's desk drawer. Even if the hard drive is broken, the forensic consultant may be able to extract its ESI. In one case, about 25 gigabytes of overlooked ESI were discovered in a hidden sector of a mail server.⁷⁴ In *Phoenix Four*, defendant Strategic Resource Corp. (SRC) ceased operations and its former principals took two of its servers to start a new business venture.⁷⁵ A year later, Phoenix sued SRC and its former principals.⁷⁶ The former principals did not search the server for relevant ESI on the belief that there was none, and told their counsel that because SRC ceased operations, there were no computers to search for ESI.⁷⁷ Yet another year later, a technician brought in to repair one of the original SRC servers "discovered about 25 gigabytes of data . . . in a dormant, partitioned" sector of the server's hard drive.⁷⁸

The partitioned sector was invisible to users because it was not "mapped."⁷⁹ The discovered documents were "central" to Phoenix's claims.⁸⁰ The court scolded both the SRC defendants and their attorneys.⁸¹ The first were negligent for telling their counsel that there were no computers to search, when they knew that some of their servers came from SRC⁸² and the attorneys were "gross[ly] neglig[en]t" for not following *Zubulake V* and searching for *sources* of ESI.⁸³ Had counsel been diligent, it should have asked about the fate of SRC's computers.⁸⁴ Nevertheless, because the defendants promptly disclosed the newly-discovered ESI, the court declined to impose sanctions.⁸⁵

The take-away from *Phoenix Four* is that counsel must inquire into the disposition of computers when companies fold, employees leave and equipment is reassigned. Similarly,

the loss or theft of a custodian's computer at a time relevant to the lawsuit should be inquired into and documented in a memo. If the computer contained ESI that was central to the issues in the lawsuit, a police report should be filed documenting the theft. Finally, even if computer is lost, counsel should inquire if its custodian preserved some of the key files on a DVD or USB drive.

In sum, counsel should document all the ESI collection activities in a memorandum to file. Relevant custody transfer issues should also be documented.

Conclusion

ESI preservation and collection for e-discovery is where the law, IT and project management meet. In a large lawsuit, where hundreds of millions of dollars are at stake, it is essential to get it right from the start. Counsel otherwise runs the risk that ESI preservation disputes will overtake the substantive issues of the lawsuit, with potentially disastrous consequences for the client's case.

Counsel must act proactively to ensure that all relevant client ESI is preserved or collected as early in the case as possible by developing a comprehensive understanding of the client's IT architecture, and by personally directing the preservation and collection measures. Even though such a strong and proactive approach creates the risk that ESI will be over-preserved, the ESI does not always have to be produced. A review of the ESI may reveal that portions of it are not relevant. But if the ESI must be produced, it will have been preserved.

Pierre Grosdidier is an associate in the Business Litigation practice group in the Houston office of Haynes and Boone, LLP. He received his Ph.D. in engineering from Caltech, and his J.D. from the University of Texas School of Law, where he served as an editor on the Texas Intellectual Property Law Journal.

The author is greatly indebted to Thomas Wisinski, Randal Girouard and Denny Miles of Haynes and Boone, LLP's IT Litigation Support Group for sharing their valuable expertise and insight regarding all the technical issues discussed in this article.

¹ *Qualcomm Inc. v. Broadcom Corp.*, No. 06-cv-01958, [2008 BL 1486](#), at **13, 17-18 (S.D. Cal. Jan. 7, 2008), *vacated in part*, *Qualcomm Inc. v. Broadcom Corp.*, [No. 05-cv-01958](#) (S.D. Cal. Mar 05, 2008).

² *Id.* at **17-18.

³ This article deals only narrowly with the preservation and collection of ESI, and leaves aside how the ESI should be processed, reviewed and produced to opposing counsel.

⁴ No. 04-cv-01199, [2008 BL 42543](#), at *2 (D. Nev. Feb. 22, 2008).

⁵ *Id.*

⁶ *Id.*

⁷ *Id.* at **1-2.

⁸ *Id.* at **2-3.

⁹ *Id.* at *3.

¹⁰ *Id.*

¹¹ *Id.* at 3–4.

¹² *Id.* at *6.

¹³ *Zubulake v. UBS Warburg LLC*, 229 F.R.D. 422, 434 (S.D.N.Y. 2004) (“*Zubulake V*”) (“[i]n cases involving a small number of relevant backup tapes, counsel might be advised to take physical possession of backup tapes”).

¹⁴ Bankr. No. 03-00817, 2007 BL 137572, at *1 (Bankr. D. Haw. Oct. 30, 2007).

¹⁵ *Id.* at *2.

¹⁶ *Id.* at **2–3.

¹⁷ *Id.* at **3–4.

¹⁸ *Id.*

¹⁹ *Id.* at *5.

²⁰ *Id.*

²¹ *Id.*

²² *Id.*

²³ *Id.*

²⁴ The Sedona Conference® Glossary: E-Discovery & Digital Info. Mgmt. 11 (2d ed. 2007).

²⁵ *Zubulake v. UBS Warburg LLC*, 220 F.R.D. 212, 218 (S.D.N.Y. 2003) (“*Zubulake IV*”).

²⁶ *Simon Prop. Group*, 2007 BL 137572, at *2.

²⁷ This conservative definition of who qualifies as a custodian is intended to be as least as broad as *Zubulake*’s.

²⁸ Counsel should use the interviews with the client’s employees to get a head start on building the list of the *opposing side*’s custodians. The employees will know who are the key players on the opposing side, and can provide e-mail distribution lists and even the names of the assistants.

²⁹ See, e.g., *Cache la Poudre Feeds, LLC v. Land O’Lakes, Inc.*, 244 F.R.D. 614, 627 (D. Colo. 2007) (citing cases discussing companies’ obligation to obtain documents in the hands of former employees).

³⁰ *Telecom Int’l Am., Ltd. v. AT&T Corp.*, 189 F.R.D. 76, 81 (S.D.N.Y. 1999); but see, *Danis v. USN Comm’ns, Inc.*, No. 98-cv-07482, at **14, 41, 51 (N.D. Ill. Oct. 23, 2000) (recommending monetary sanctions against company CEO who displayed “extraordinarily poor judgment” in delegating supervision of preservation program to inexperienced in-house counsel, who was in turn negligent and ineffectual).

³¹ Files are “dispersed” when they are saved in scattered and unrelated folders on a hard drive. The consequence is that these files are securely preserved only when the entire drive is forensically copied, a costly and wasteful practice.

³² *Telecom Int’l.*, 189 F.R.D. at 81.

³³ 244 F.R.D. 614, 616–17 (D. Colo. 2007).

³⁴ *Id.* at 624–25.

³⁵ *Id.* at 629–30.

³⁶ *Id.* at 625, 628.

³⁷ *Id.* at 630.

³⁸ *Id.*

³⁹ *Id.* Despite the severity of its admonitions, the court only fined Land O’Lakes \$5,000 plus the costs of deposing its in-house counsel. *Id.* at 638.

⁴⁰ No. 98-cv-07724, at *2 (S.D.N.Y. Mar. 30, 2000). MIS: Management Information System; another term for IT.

⁴¹ *Id.*

⁴² *Id.*

⁴³ *Id.*

⁴⁴ *Id.*

⁴⁵ *Id.*

⁴⁶ *Id.*

⁴⁷ *Id.*

⁴⁸ *Id.* at *1; see also *Zubulake V*, 229 F.R.D. at 434 ([o]ne of the primary reasons that electronic data is lost is ineffective communication with information technology personnel”).

⁴⁹ *Johnson v. Kraft Foods, N. Am., Inc.*, 238 F.R.D. 648, 655 (D. Kan. 2006); see also *Mosaik Techs. Inc. v. Samsung Elecs. Co., Ltd.*, 348 F. Supp. 2d 332, 336–37 (D.N.J. 2004) (invoking L. Civ. R. 26.1(d), which requires, among other things, that counsel investigate how clients’ computers store digital information).

⁵⁰ *Zubulake V*, 229 F.R.D. at 432 n.73 (citing *Zubulake v. UBS Warburg LLC*, 217 F.R.D. 309, 324 (S.D.N.Y. 2003) (“*Zubulake I*”) (emphasis added); see also *Id.* at 432 (“counsel must become fully familiar with her client’s document retention policies, as well as the client’s data retention architecture”).

⁵¹ See, e.g., *Columbia Pictures, Inc. v. Bunnell*, 245 F.R.D. 443, 446 (C.D. Cal. 2007) (ruling that RAM data was electronically stored information under the Federal Rules, despite its short-lived nature, and subject to discovery under the facts of the case).

⁵² See, e.g., *Cache la Poudre*, 244 F.R.D. at 621 (defendant automatically deleted e-mails older than 90 days).

⁵³ The Sedona Principles 105 (BNA Books, 2d ed. 2007) (Comment 5.h, “[a]bsent specific circumstances, preservation obligations should not extend to disaster recovery backup tapes created in the ordinary course of business”) (emphasis added). The Sedona Principles define best practices for ESI production (www.thesedonaconference.org).

⁵⁴ *Zubulake IV*, 220 F.R.D. at 218 (“[a]s a general rule, that litigation hold does not apply to inaccessible backup tapes (e.g., those typically maintained solely for the purpose of disaster recovery), which may continue to be recycled on the schedule set forth in the company’s policy. On the other hand, if backup tapes are accessible (*i.e.*, actively used for information retrieval), then such tapes *would* likely be subject to the litigation hold”) (emphasis in original); but see qualifier *infra*.

⁵⁵ *Id.*

⁵⁶ Disaster recovery tapes normally save application and user files and do not save system files. If a server drive “crashes,” the operating system must be reinstalled on the new drive before application and user files can be restored from the disaster recovery tapes.

⁵⁷ 2007 BL 137572, at *3.

⁵⁸ *Zubulake IV*, 220 F.R.D. at 218. Likewise Comment 5.h of the Sedona Principles qualifies its rule regarding the continued recycling of back-up tapes with “[a]bsent specific circumstances.”

⁵⁹ *Zubulake IV*, 220 F.R.D. at 218.

⁶⁰ A third reason to proceed cautiously is that it may be difficult to know what is on the back-up tapes. Some IT groups keep their back-up tapes neatly aligned and labeled on a shelf. Other groups have bins that contain hundreds of unlabeled tapes including everything from DEC TK-50s to the latest LTOs. Even though there is generally no reason to believe that these large tape collections contain relevant ESI, they must nonetheless be preserved in case the court orders sampling of the tapes.

⁶¹ The disks are actually disk arrays that function with redundancy. Only under extraordinarily unfortunate circumstances would two mirror disks crash at the same time and result in the permanent loss of data.

⁶² Therefore, if a server disk crashes on Wednesday, the restoration will rely on the previous Saturday’s full back-up, supplemented with the Monday night and Tuesday night incremental back-ups. All data created or saved on the server between the Tuesday incremental back-up and the crash will be irremediably lost.

⁶³ In most instances, that tape will never be used again. Indeed, by the time that the data is so obsolete that the tape can be recycled, e.g., two or three years, the tape will be old enough to be judged unreliable. Moreover, the technology will have evolved, and the amount of data to be stored will be so much greater that a new tape will be a better solution. Some users now even archive to hard drives.

⁶⁴ Likewise, a file that is created in the morning and deleted before the end of the same day will not be captured by the daily incremental back-up, which typically runs at midnight and captures only active data.

⁶⁵ See, e.g., *Wiginton v. CB Richard Ellis, Inc.*, No. 02-cv-06832, [2003 BL 1515](#), at *4, (N.D. Ill. Oct. 24, 2003) (noting that a party need not go to “‘extraordinary measures’ to protect all potential evidence” nor “preserve every single scrap of paper in its business”).

⁶⁶ It is a good idea for counsel to verify that the purchase is made, and not delayed or blocked by bureaucracy.

⁶⁷ Whatever ESI collection-related work is done by the IT group should be done under a work order so the internal cost of the collection can be tracked.

⁶⁸ The Sedona Conference® Glossary: E-Discovery & Digital Info. Mgmt. 23 (2d ed. 2007).

⁶⁹ Not every media can be practically imaged. Personal computers, portable hard drives, and USB drives are easily imaged. Servers are not because of the size of the data set that must be collected. Moreover, there is generally no need to image complete servers. Forensic copies of relevant server file folders preserve all metadata and are generally sufficient. However, forensic copies of server file folders do not preserve evidence of disk wiping. If counsel suspects that server files have been tampered with, the proper course of action is to request a forensic audit of the server.

⁷⁰ As discussed, one of the reasons why back-up tapes must be preserved is to protect against employees deleting files in the personal or group shared drives. If this happens, the back-up tapes are the only source of the files.

⁷¹ The practice should be strongly discouraged by employers as it complicates e-discovery and increases its cost. The better solution is to equip employees with laptops, or to grant them cloud-computing access to company servers.

⁷² E-mails are very important not only in and of themselves, but also because of the attached files that are sent with them. Even if a custodian deletes a nettlesome memo or spreadsheet from a disk folder, there is a good chance that the deleted file will be found somewhere as an attachment to an e-mail.

⁷³ 229 F.R.D. at [432](#).

⁷⁴ *Phoenix Four, Inc. v. Strategic Res. Corp.*, No. 05-cv-04837, [2006 BL 130960](#), at *2 (S.D.N.Y. May 23, 2006). The 25 gigabytes corresponded to approximately 2500 boxes of documents. *Id.*

⁷⁵ *Id.* at **[1-2](#).

⁷⁶ *Id.* at *[2](#).

⁷⁷ *Id.*

⁷⁸ *Id.*

⁷⁹ *Id.*

⁸⁰ *Id.* at *[6](#).

⁸¹ *Id.*

⁸² *Id.*

⁸³ *Id.* at **[5-6](#).

⁸⁴ *Id.*

⁸⁵ *Id.* at *[7](#).

Alternative Dispute Resolution

Motion to Stay

Former Employee’s Case Dismissed on Motion to Stay Pending Arbitration

[Franz v. Allegheny Inv., Ltd., No. 1:08-cv-01983, 2010 BL 28871 \(N.D. Ohio Feb. 11, 2010\)](#)

On February, 11, 2010, the U.S. District Court for the Northern District of Ohio dismissed an action brought against a financial services firm for its alleged failure to extend defense coverage in a Financial Regulatory Authority (FINRA) arbitration.

Factual Background

In the fall of 2005, a church notified defendant Allegheny Investments, Ltd. (Allegheny) of a claim against it and George Franz III, one of its employees. At the time, Westchester Insurance covered the claims against Franz and the firm under an errors and omissions policy. Allegheny’s personnel evaluated the claim and concluded that Franz had acted properly. Despite this conclusion, Franz resigned from Allegheny in November 2005. When the church instituted the FINRA arbitration in October 2007, Franz was not provided with defense coverage and was forced to pay for his own defense.

Franz brought the current action against Allegheny seeking payment for the costs incurred in defending the FINRA arbitration. In his complaint, Franz alleged that the firm had refused to verify the existence of insurance coverage for him, misrepresented the coverage available to Franz and the correct amount of the deductible, concealed the applicable policies, refused to provide proof of insurance and refused to provide Allegheny’s claim file. Franz claimed that Allegheny’s misconduct forced him to retain his own counsel and expert witness. He sought a declaration that Allegheny was responsible for his defense and coverage costs. The action was stayed pending the FINRA arbitration. In December 2009, during a teleconference, counsel informed the district court that the arbitration panel had issued an arbitration award absolving Allegheny but finding Franz liable for the church’s claim.

On January 15, 2010, Allegheny moved to stay Franz’s suit, contending that Franz was required to arbitrate his defense coverage claims in accordance with the Form U-4 Uniform Application for Securities Industry Registration (Form U-4) that he had signed in October 2001. Form U-4 states that an applicant agrees to arbitrate “any dispute, claim or controversy that may arise between [the applicant] and [the applicant’s] firm, or a customer, or any other person, that is required to be arbitrated under the rules, constitutions, or by-laws of the [self regulatory organization].” Franz opposed