

Litigation Support

Document Forensics and Legal Holds

Autonomy and Interwoven help 75% of the Global 100 and 73% of the AmLaw 100 get their ducks in a row.



The Fastest Growing EDD Provider to the AmLaw 200 Meets the De Facto Standard in Legal Information Management

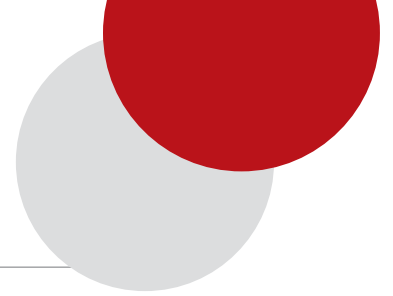
Autonomy can now link **1,400** law firms with the data inside **17,000** corporate clients using a single, powerful platform. For the first time, outside counsel can Discover-in-Place, allowing them to access and analyze corporate data of any kind, including audio and video. This continuous chain streamlines the processes that occur between a law firm and its clients.

Find out how at www.autonomy.com/imanage.

“The acquisition of Interwoven is a master stroke.”

—Seymour Pierce, January 2009





One of our authors touches on the collaborative process that is undertaken by her firm's records, litigation support and IT departments in managing legal holds and subpoenas directed to the firm. Not surprisingly, this white paper reflects the combined efforts of ILTA's Litigation Support, Records Management and Law Department Peer Groups.

The complexities of pending litigation can't be confined to one department in the firm or law department; processes, systems and well-trained people will contribute to the effective management of time and resources and the ultimate outcome.

Mary Pat Poteet of DLA Piper LLP is ILTA's Vice President for the Litigation Support Peer Group. She provided direction for the

development of content in this publication, the focus of which is twofold: **forensics** and **legal holds**. **Sally Letteri** of United States Steel Corporation, Vice President for ILTA's Law Department Peer Group, reached out to her constituency, and the great contributions from our corporate law departments are reflected in the bylines you'll find. And **Charlene Wacenske of Morrison & Foerster LLP**, our Peer Group Vice President in the Records arena, provided her own expertise for managing legal holds. Read and enjoy.

Randi Mayes
Editor-in-Chief

In This Issue

4 OVERCOMING DATA ENCRYPTION FOR FORENSIC IMAGING AND COLLECTIONS

by **Chris Pavan and Nick Ringold, 42 LLC**

By understanding how encryption works and the current techniques used in decryption, retrieving encrypted data becomes manageable.

8 WHEN IS FULL-BLOWN FORENSIC COLLECTION NECESSARY?

by **Tom Morrissey, Purdue Pharma LP**

It is possible that we are confusing "forensics" with "process," and we are substituting forensic tools for true forensic methods.

12 WHEN "DELETED" DOESN'T MEAN "GONE"

by **Mike Sinnwell, Belin Lamson McCormick Zumbach Flynn**

Our author mitigates the enigmatic nature of computer forensics by stripping out the technical jargon to examine the process.

STATEMENT OF PURPOSE

ILTA is the premier peer networking organization, providing information to members to maximize the value of technology in support of the legal profession.

ABOUT ILTA

Providing technology solutions to law firms and legal departments gets more complex every day. Connecting with your peers to exchange ideas with those who have "been there done that" has never been more valuable. For over three decades, the International Legal Technology Association has led the way in sharing knowledge and experience for those faced with challenges in their firms and legal departments. ILTA members come from firms of all sizes and all areas of practice, all sharing a common need to have access to the latest information about products and support services that impact the legal profession.

16 DISASTER RECOVERY OR DISCOVERY DISASTER?

by **Michael Iwan, Dorsey & Whitney LLP**

Backup tapes are not necessarily an appropriate or efficient means of preserving documents and data for litigation. Excessive reliance on backup tape preservation has the potential to create a false sense of security for a litigant.

20 LEGAL HOLD AND SUBPOENA COMPLIANCE COORDINATION

by **Charlene Wacenske, Morrison & Foerster LLP**

Many firms struggle with how to effectively manage legal holds and subpoenas directed towards them. Find out how one large firm coordinates the effort.

22 BEST PRACTICES FOR LEGAL HOLD PROCESSES

by **Jeffrey J. Beard, Esq., Daticon EED**

Unlike paper, electronically stored information (ESI) is more easily lost, modified, overwritten and deleted unless active steps are taken to manage this process throughout the life of the matter.

28 THE EFFECTS OF LITIGATION HOLDS ON THE CORPORATE LAWYER

by **Cindy MacBean, General Motors Corporation Legal Staff**

The time and effort to establish teams to respond to inquiries, develop documents across functional areas and obtain a consensus of the content within a legal department is considerable.

Overcoming Data Encryption for Forensic Imaging and eDiscovery Collections

Due to the ever-growing security requirements imposed on organizations, data encryption is becoming commonplace. This makes the task of retrieving data, which is potentially relevant for legal purposes, difficult, as the nature of encryption is to prevent access to data. However, by understanding how encryption works and the current techniques used in decryption, retrieving encrypted data becomes manageable.

ENCRYPTION IS EVERYWHERE

Encrypting data has become a requirement for many, if not all, organizations that store electronic information. This is due to a variety of different regulations and laws set forth by GLBA, SOX, HIPAA, PCI DSS, FIPS 140-2, and many state statutes. Many, if not all, of these laws and regulations have failed to account for legal requirements pertaining to discovery. Although they typically provide a mechanism to recover data, it is not always “forensically sound,” which means the original source of information is duplicated to best represent the data without modifying or destroying any of the original data or its metadata. It also means it should be possible to completely reconstruct the sequence of events on a computer purely from the collected data. The end goal is to have an exact physical representation of the entirety of the data in a human-interpretable form.

A DATA ENCRYPTION PRIMER

Data can be encrypted in many different ways, on a number of levels, and depending on the way it is

encrypted, the method for duplication will vary. Here, we will discuss three major types of encryption: physical disk (often referred to as whole disk encryption), individual or logical file and individual record.

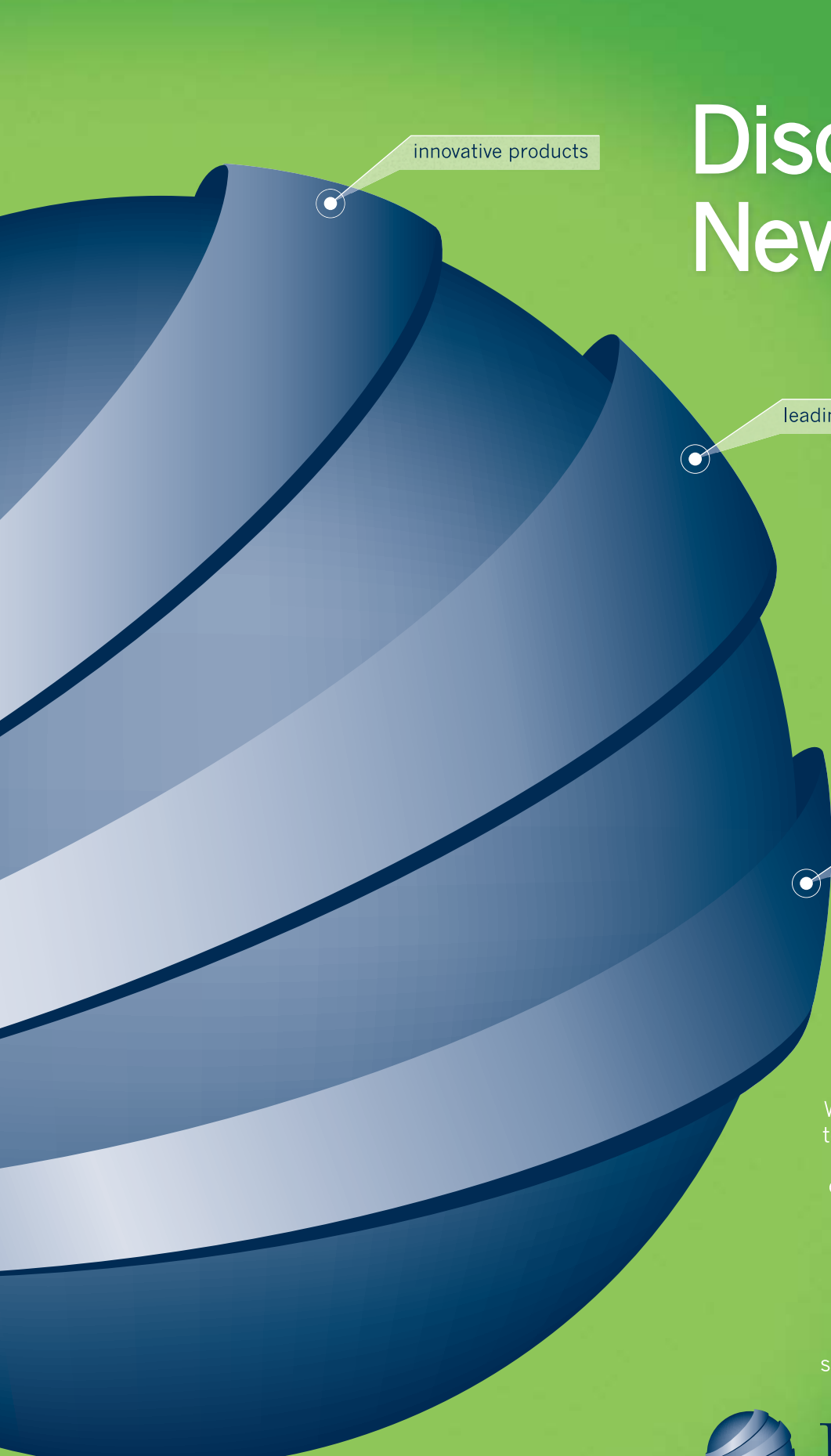
Physical disk encryption is a very common and secure way for protecting all types of data contained on a hard drive. The data is encrypted at the lowest level of the drive, which prevents the data from being read without the proper credentials or hardware tokens. When the computer boots, the user is prompted for a password or asked to insert a USB device and enter a PIN.

Regardless of the method of authentication, without the proper credentials, you will be unable to boot the computer or access the data. This also prevents anyone from connecting the hard drive to another computer in order to access the data. For example, if the drive were lost or stolen, the data could not be compromised without the proper credentials. Although physical disk encryption is a good way to protect hard drive data from being accessed offline, the data is vulnerable once the computer is successfully booted.

Logical file encryption, on the other hand, will not protect all of the data on a hard drive, but it will protect individual user-encrypted files. How difficult and time consuming the decryption will be depends on the type of encryption and the technical controls employed.

In environments with extremely sensitive data contained in specific individual files, logical file encryption protects the data from anyone who manages to gain access to the encrypted file itself. For instance, it is common practice to encrypt sensitive documents so that the content remains protected even if it is accessed or viewed by someone other than authorized individuals.

Discover the New Esquire.



innovative products

leading technologies

professional staff

Discover What We're Made Of.

When we set out to create the new Esquire, we set our sights on redefining litigation support. We built for the long haul, bringing together the best people, products and cutting-edge technologies to create the most complete solution in the world. From court reporting to eDiscovery to legal staffing, we have the experience and depth to deliver any support service, anywhere in the country. Strength, expertise and a commitment to service – that's what we're made of.



ESQUIRE
an Alexander Gallo Company

EsquireSolutions.com

The image below is a side-by-side example of a logical file in its encrypted and decrypted states. The file was originally encrypted with one of the many tools that encrypt files with the AES-256 algorithm. The left side of the image shows the data in an encrypted state, while the right side is unencrypted. When performing a keyword search for the term “Copyright,” the file on the right would be responsive to the keywords, while the one on the left would not. This presents another layer of complexity to eDiscovery collection, processing and review.

```

0000 37 7  00 00 7z4".....}...
0010 00 0  08 85 .....X.....3A..
0020 00 2  0a 8f .#..i+i6...43!..
0030 e5 5  19 d6 .â..r2..b90-000
0040 a5 7  32 4e VZUc...j0\I..I-N
0050 c6 e  56 91 #Sst-Ph0U:â.r-
0060 aa 3  14 4a *1IH-@I-0-ÉAaJ
0070 44 0  06 c2 D-u-yivEaITur..Å
0080 b2 9a 7 2e .+gââ0m- ->[p>.
0090 68 2e 3 9d h* (:âid <-u00p-
00a0 4c 82 3 02 L-40y-g-w00xââ0
00b0 5c 04 1 5f \-0x006)~Å(H-PD_
00c0 4f 92 1 bb 0-0z 7A-~4~(0I »
00d0 bc 12 1 04 h-00VÅSVE<)*cP .
00e0 d0 40 1 dd D0~+0âiq~*4f-0f
00f0 2d 23 1 10 -#..0Q-P-0-â2-±-
0100 9e dr 1 d2 -UN-0JJe9-\-00=0
0000 47 4e 42 4c GNU GENERAL PUBL
0010 49 4f 72 73 IC LICENSE..Vers
0020 69 6f 39 31 ion 2, June 1991
0030 20 0f 20 28 ....Copyright (
0040 43 2f 46 72 C) 1989, 1991 Fr
0050 65 6f 75 6e ee Software Foun
0060 64 6f 0d 0a dation, Inc. ..
0070 35 3f 55 20 59 Temple Place
0080 2d 2f 1f 73 - Suite 330, Bos
0090 74 6f d 31 ton, MA 02111-1
00a0 33 30 5 72 307, USA....Ever
00b0 79 6f 4 65 yone is peraitte
00c0 64 20 4 69 d to copy and di
00d0 73 74 4 69 stribute verbatl
00e0 6d 20 3 69 m copies-of thi
00f0 73 20 4 65 s license docum
0100 6e 74 e 67 nt, but changing

```

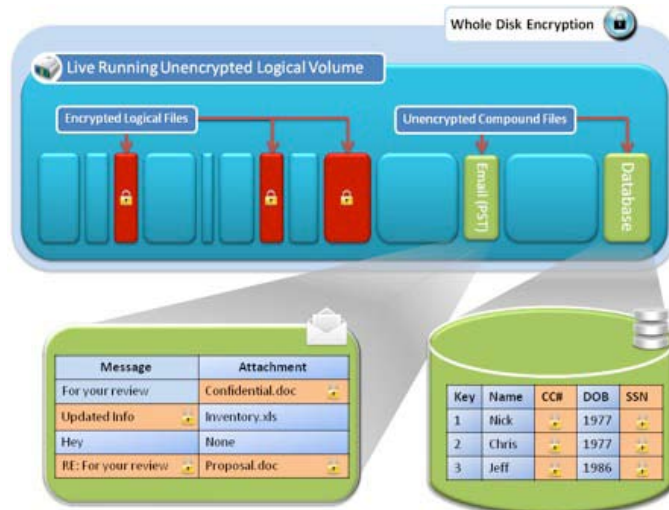
The third type, individual record encryption, is typically used for protecting database data. The most sensitive database information is encrypted, while the other data is in plain text. Some examples are credit card numbers and Social Security numbers. Organizations storing sensitive data are required by various security regulations and standards to impose this level of encryption. If a malicious individual or process gained access to one of these protected records directly, the information would be useless without the algorithm, encryption key and passphrase or token.

VISUALIZING THE DIFFERENT TYPES OF ENCRYPTION

Below is a block diagram showing how different encryption types can be used. The outermost layer, the physical disk, is protected with “whole disk encryption.” The data is inaccessible unless decrypted, which generally occurs during the boot process. Once the system is booted and running, the data on the next layer, which is the logical volume of the disk¹ labeled “live running unencrypted volume,” can be accessed.

Inside the logical volume are the individual files. Individual files can be encrypted by a wide variety of software applications utilizing different algorithms. The files shown in blue blocks are files that have not been encrypted individually and can be viewed natively with their associated software applications. The “encrypted logical files,” shown in red, must be decrypted prior to being viewed. Additionally, there are “unencrypted compound files,” which can contain individual encrypted records internal to the logical file. This can

include encrypted e-mail messages, attachments or individual fields in a database.



OVERCOMING WHOLE DISK ENCRYPTION

Forensic imaging relies on a standard protocol of removing the hard drive from a system after it has been powered down, connecting that hard drive to a forensic write-protection device and copying the drive using a tool such as EnCase² or dd. These tools create a bit-for-bit image of the entire drive. This particular method works in most cases, but not with whole disk encryption, which presents a significant challenge for organizations that are required to produce data as part of a legal proceeding.

The image above shows that the user can access their files once the system is booted and logged in, but if the disk is forensically imaged without a means to decrypt the data, the forensic examiners and the litigation support staff will not be able to access the user’s data. However, if we boot the system and use the same process that facilitates the encryption / decryption to access the logical volume, we can obtain a forensic copy of the “unencrypted logical volume.”

When using a forensic tool like EnCase, it is clear that the data on a hard drive utilizing whole disk encryption is inaccessible. Although EnCase and other forensic tools can decrypt the data on some drives where whole disk encryption is used, attempting to decrypt the data at a later date is not advisable. It is far easier to acquire the data from the already decrypted logical partition than to rely on decryption through a forensic tool, particularly if the encryption form is unsupported by the tool. If we were to examine the same drive in a booted state, we would see that the data is now unencrypted.

There are a number of ways to access a booted system in order to directly copy an unencrypted logical volume. Enterprise forensic tools such as Helix 3 Enterprise³ and EnCase Enterprise have made it possible for examiners to collect data from live running computer systems via an organization’s network

infrastructure. Because the computers are running, the data can be collected in unencrypted form from the logical drive (e.g., C:\). Although some drivers may present both the physical drive and logical volume in an unencrypted state, it is generally safer to collect logical volumes and not physical disks.

Although enterprise class forensic tools are very powerful, they are not always deployed, which requires another method for forensic image creation. In the absence of such a tool, the examiner must work with a system administrator to gain access to the booted system. Once the examiner has access to the computer (with administrative privileges), it is then a matter of using a tool such as FTK Imager⁴ to create an image of the system. Likewise, an examiner can use EnCase to create forensic images directly from a live computer, again collecting logical volumes and not physical disks.

ISSUES WITH IMAGING LIVE RUNNING SYSTEMS

When making a forensic image of a running computer, it is important to remember that data is constantly changing. If the computer is in use, then there is no control over what data is changing. This can result in considerable data corruption in the forensic image, which can occur as a user continues working during the process, including creating and modifying different files with applications like Microsoft Outlook, Excel and Word. This also applies to the logical collection of files based on forensic applications. Because the forensic tools are looking at the raw data on the drive via a “snapshot” of the file system, they fail to account for the ongoing modification of data during the collection.

A more specific, and often very common, example is a PST⁵ file. As e-mail messages are sent and received, the PST file grows in size and the structure of the file changes. As sophisticated as forensic applications are, they do not account for changes to the live running system. This presents a problem when trying to access the PST file after the collection. The file must be “repaired” so that the file structure can be read and the messages extracted. Although PST files can often be repaired through the use of a vendor-supplied tool, other file types are not so easily recovered.

On the other hand, if the examiner has direct control over the computer, he can ensure that none of the user-based data is being accessed or changed during the imaging process. By taking physical control over the subject system, keeping it disconnected from any networks and quitting all unnecessary programs and services, the data is preserved in as pristine a state as possible given the circumstances. This can also be accomplished with an enterprise-class tool if the user

quits all applications and logs out of the system. If this is done at the end of the day and the collection is performed after hours, the examiner will have more time to complete the process without impacting the user and the integrity of the collected data.

Regardless of the method used, small changes will be made to the system. The examiner should document the process and be prepared to articulate what changes that process may have made to the computer. But, provided that the examiner used sound methodology, no unexpected changes should have occurred to the system by the examiner’s process. Again, because it is very difficult, if not impossible, to account for the user’s actions during the imaging process, it is advisable to conduct the imaging in as controlled an environment as possible.

LITIGATION SUPPORT CAN OVERCOME ENCRYPTION

While whole disk encryption is reasonably easy to deal with, logical files and database records are far more difficult to decrypt and often require custom-built applications. The different elements of litigation support have to come together in order to successfully overcome the different types of encryption used.

Finally, FRCP Rule 34(a)(1)(A) requires parties to produce “[data] stored in any medium from which information can be obtained either directly or, if necessary, after translation by the responding party into a reasonably usable form.” The expectation is that if the user has stored the data in a manner in which they are able to retrieve it, the data is subject to discovery. Whether logical files or database records, the data is still accessible to the user (which makes them a custodian) in an intelligible form, so that data should be presented in an intelligible form for litigation. It is unreasonable to ignore or fail to properly process encrypted data. Although there are exceptions, at a minimum, the producing parties should identify all potentially relevant encrypted data, and be prepared to decrypt that data for discovery. **ILTA**

ENDNOTES

¹ It is important to note that the logical volume is not visible on a wholly encrypted disk unless the disk is unencrypted.

² EnCase is an industry standard forensic analysis tool created by Guidance Software Inc. (NASDAQ: GUID, <http://www.guidancesoftware.com>).

³ Helix 3 Enterprise is a forensic tool created by e-Fense (www.e-fense.com).

⁴ FTK Imager is a forensic acquisition tool created by Access Data (www.accessdata.com).

⁵ A PST file is used by Microsoft Outlook and is a repository for e-mail messages, calendar and journal entries.



When Is Full-Blown Forensic Collection Necessary?

According to *The Sedona Conference Glossary: E-Discovery & Digital Information Management (Second Edition www.thesedonaconference.com)*, forensics is:

The scientific examination and analysis of data held on, or retrieved from, ESI in such a way that the information can be used as evidence in a court of law. It may include the secure collection of computer data; the examination of suspect data to determine details such as origin and content; the presentation of computer based information to courts of law; and the application of a country's laws to computer practice. Forensics may involve recreating 'deleted' or missing files from hard drives, validating dates and logged in authors/editors of documents, and certifying key elements of documents and/or hardware for legal purposes.

Essentially, the forensics process involves highly specialized investigators, or criminalists, locating evidence that provides conclusive proof when tested under laboratory conditions. This definition applies to

all forms of evidence generally associated with criminal activity. There are different types of forensic practices that the law utilizes — forensic pathology, forensic accounting and forensic economics. But these are not used in every matter, only where warranted or required by law or a court.

“Computer forensics” refers to the investigation of activity on any device that contains, is managed by, or used by a computer. This generally refers to workstations and servers, but can include handheld devices, networked printers, fax/scan devices, portable music players, removable storage devices and even third-party hosted applications. A forensic collection is generally warranted to be performed when inappropriate and/or illegal activity is suspected. The current mindset of the legal community has diverted, in my view, away from the true definition of “computer forensics.” In the current landscape, “forensics” has come to mean using forensic methods and tools for collection and preservation in ordinary civil litigation.

DETERMINING THE NEED FOR FORENSICS

It is possible that we are confusing “forensics” with “process,” or doing something in a documented, repeatable manner that can

be relied upon to show what was done, by whom and when. And we are substituting forensic tools for true forensic methods, that is, using a forensic imaging tool to capture drive contents, but not keeping up with the paperwork.

Further, it is possible that true computer forensics should be reserved only for a criminal or potentially criminal matter (civil misappropriation of trade secrets, data security violations, civil fraud involving computer systems). Corporations and law firms alike can utilize forensic imaging tools and methods in several areas not associated with discovery in civil matters. These types of situations might include (a) employee dismissal (data retention) (b) policy violations or criminal acts (Website visits, download/upload files.) and (c) Network Intrusion (tracking what happened.)

My short answer to the question posed in the title “When is a full-blown forensic collection necessary?” is “Almost never.” Unless there is a pending criminal or serious federal investigation pending, a full-blown forensic collection is not warranted.

It is widely acknowledged that the smoking gun sought in the majority of civil cases will not be found in the slack files or deleted data. A surfeit of relevant and responsive data will be the result of statements made in e-mail messages, instant messages, or in externally circulated corporate intranet content statements, or in internal memos.

Alternatively, in certain extreme cases, the use of forensic collection tools and methods might be useful tools in targeted collections of key custodians to litigation to show the court you took the preservation and collection seriously.

Additionally, there are risks associated with both improper and proper applications of forensic tools and methods. For instance, forensic data collection can lead to an increase in the amount of data collected, and in the long run, may well increase the overall cost of discovery due to the over-collection of irrelevant and non-responsive data. What do you do with all the data that is now in your care, custody and control, and that could be construed as improper use of corporate assets?

Since many “experts” these days are concerned with the large volumes of data being collected for discovery and the lack of any reliable relevancy search tool, it is recommended that firms and corporations only collect the potentially responsive files that are in scope. If the decision is to “go forensic” with everything, then somebody has to search that data no matter how much is collected. The following excerpt highlights the issue that arises when the collection process is not carefully thought out.

Excerpted from “Digital Discovery & e-Evidence Report,” Are We Entering the Post-Forensic Era? (April 1, 2009) By Jake Frazier, Esq. from EMC.

Have We Gone Too Far?

Working at an e-discovery service bureau prior to the revisions to the Federal Rules of Civil Procedure, my company was hired by a defendant-corporation in a civil case. A team of more than a dozen forensic technicians was mobilized to over 30 cities to create and collect over 1,000 forensic images of individual workstations, servers, and the like.

Forensic copies were made, so every system file and every bit of “empty” space on each hard drive was collected, and put into a proprietary compressed evidence file. The bill was well over \$1 million to do the collection alone and pay for travel expenses.

Once the processing started, technicians certified by the software company that owns the collection software were required to open and extract the documents from these copies. This was a painstaking process and took weeks. Only then could the documents be put into a review tool such that the e-discovery process could resume.

To my recollection, there was no suspicion of wrongdoing or intentional deletion of files, no was recreating the actions of the users particularly important. However, this was the “best” way to collect evidence at the time.

It is likely that this example and many others like it were the impetus for revising the Federal Rules of Civil Procedure, especially Fed. R. Civ. P. 26(b)(2)(b), which now states:

(B) Specific Limitations on Electronically Stored Information. A party need not provide discovery of electronically stored information from sources that the party identifies as not reasonably accessible because of undue burden or cost.

Without diving deeply into the issue of what constitutes “undue burden,” it is not unreasonable to assume that objection to the creation of forensic copies of hard drives—where there has been no showing of the special need for doing so, is at least a reasonable argument to be made during the Fed. R. Civ. P. 26 (f) meet and confer process, or if before that process, perhaps as a best practice, or to be discussed in preservation communications earlier on in a case.

Otherwise, the only conclusion is that making a forensic copy of any hard drive that contains ESI that “may be relevant to future litigation” is in order, and that is clearly cost prohibitive.

This situation highlights that using physical forensic acquisition of a drive, or drives, is essentially over-collection unless you have some very specific reasons to make such a collection. An unintended consequence is that you can potentially capture irrelevant, private information (See *White vs. Graceland College Center for Professional Development and Lifelong Learning*, 2009 U.S. Dist. Lexis 22068 (D.Kan.-Mar.2009.) You may also capture contraband, which creates criminal liability for the company. (Any forensic examiner with roots in the law enforcement community will search for the NIST Child Pornography hash signatures in the collection, if for no other reason than to protect him/herself.)

THE PAPER CONNECTION

To frame my opinion, I'd like to take a journey back to the "old days" (the 1980s and 1990s).

In the years before the current "Amendments to the FRCP" were even being considered, if a large litigation (Class Action) were filed, and a corporation had to defend their interests, they would go out and hire a law firm. The law firm would work to determine the issues and map out the scope of the discovery request(s) and, if needed, work to choose a vendor via RFP to help with document processing. It was a time when paper was king and coding shops reigned supreme. Corporate employees were interviewed and "documents" were gathered. Teams of junior associates and paralegals would track and index the location of the files collected and associate them with the boxes and folders. Interrogatories were asked and answered. Firms and their vendors would then copy, scan, Bates Stamp, OCR, code, review and redact the documents. Productions of paper documents, and later images, which were determined relevant and responsive, would be made. Depositions were taken and exhibits entered. Before ESI became a common acronym, there was paper.

For trial, I confirmed the source for each document based on the collection logs or the deposition exhibit list and added them to the production logs. I cross-referenced them to the depositions and maintained the indexes of the interrogatory responses. Attorneys offered them into evidence at deposition and at trial. I logged and tracked the documents withheld as privilege, objectionable or as confidential.

As we fast forward to current thinking around forensics, there is merit in thinking of the collection of electronic data in much the same way we dealt with paper. Yes, there is metadata. Tools that track changes are great and can identify all the changes made to a document, but a legal case, for the most part, will not turn/hinge on forensics. The case will be decided on an organization's process of collection, retention, tracking and documentation about how the evidence is tracked and managed.

IT'S ALL ABOUT THE PROCESS

My grandfather used to say, "It ain't the clothes that make the man. It's the peg they're hanging on that counts." In the current environment, your discovery peg is the process you develop. The collecting and gathering of files (e-documents) should follow the same process as that of gathering paper —

log and track everything. Know where it came from and keep it. Apply retention based on your policies. Much of this process is records management 101, just with a twist. True, electronic files can be altered more easily than paper, and your collection and tracking processes need to address that fact. There are many good tools on the market and vendors who can hash and log the documents as part of a sound collection process.

“ . . .using forensic physical acquisition of a drive, or drives, is essentially over-collection unless you have some very specific reasons to make such a collection.”

FORENSICS CAN HELP IN THE DISCOVERY PROCESS

Instead of using the "forensic collection" label, simply use good data collection procedures that include applying sound forensic procedures to the process. Forensics technicians are similar to the best litigation paralegals who know how to collect, log and track data without modifying it. They can even track and log the data about the data and not alter or modify the files. Forensic technicians have good attention to detail and can validate for the lawyers and the court that information has been collected correctly. They can provide guidance to legal and IT teams on how to collect documents in a manner pleasing to lawyers and the courts, with documented and repeatable methods for collecting data that will stand up to court scrutiny. Again, the process is the peg on which the case hangs. **ILTA**

This article represents the work and opinions of the author and does not constitute official positions of Purdue Pharma LP or any other organization.



{ Well-rounded e-Discovery. }

From data collection through processing and hosted review, TechLaw Solutions incorporates impactful services that encompass the entire lifecycle of your e-Discovery project, such as near-duplicate detection, email threading and foreign language capabilities. And with more than 25 years of experience under our belt, we deliver what you need to make your project successful: superior project management and innovative technology to save time and money. *Join our circle of satisfied customers. Make TechLaw Solutions*

your e-discovery partner today.



TechLaw
>>> SOLUTIONS

Your e-Discovery Partner

CALL 800-TECHLAW (832.4529) | WWW.TECHLAWSOLUTIONS.COM

When “Deleted” Doesn’t Mean “Gone”

By now we all understand that deleted doesn’t really mean gone forever. While it used to be known only among the tech savvy, now, it’s considered common knowledge within our profession.

Indeed, firms now use this fact to support their client’s position, often by enlisting the skills of a forensic computer specialist. Because this specialist’s processes can seem enigmatic to the legal professional, we’ll strip out the technical jargon and examine how this mysterious process called computer forensics works.

FILE STORAGE 101

Understanding computer forensics requires a basic understanding of how computers store data. First, it’s important to know that different operating systems handle data storage differently. Microsoft uses various flavors of a principle that has been around since 1977, when its File Allocation Table (FAT) was introduced. More recent versions of Windows utilize a Master File Table (MFT) found in NTFS (Windows NT File System). Unix-based machines typically utilize the Unix Files System (UFS) and use the principle of a Superblock. Novell Netware servers that use Novell Storage Services (NSS) utilize a combination of Balanced Trees and the Directory Entry Table (DET). Finally, Apple computers frequently use the Hierarchical File System (HFS), which makes use of a Volume Bitmap.

While each operating system handles data storage differently, conceptually, each simply tells an operating system where to find data on physical media. For the purpose of simplification, the basic concepts of a file allocation table will be referred to and used in this article instead of specific details of each operating system type.

FAT = TOC

It might be helpful to think of a file allocation table as the table of contents in a book. It tells the computer system where to find the data on the media, just as the table of contents would tell a reader where to find information in a book. Deleting a file from the media replaces the data entries in the allocation table and sets the entry to reflect that the space is available for use (Eckstrom 2007). However, even though a blank entry replaces the table of contents entry, it still retains the page number information, which indicates that the space is available for use by the computer. In other words, when this update to the allocation table occurs, the data continues to reside on the media untouched, just as the page in the book would remain untouched if only the table of contents were modified.

WHERE DELETED DATA HIDES

Until it is overwritten by other data, the data will continue to reside on the media. When this overwrite occurs is based primarily on two factors: activity and time. The more frequently

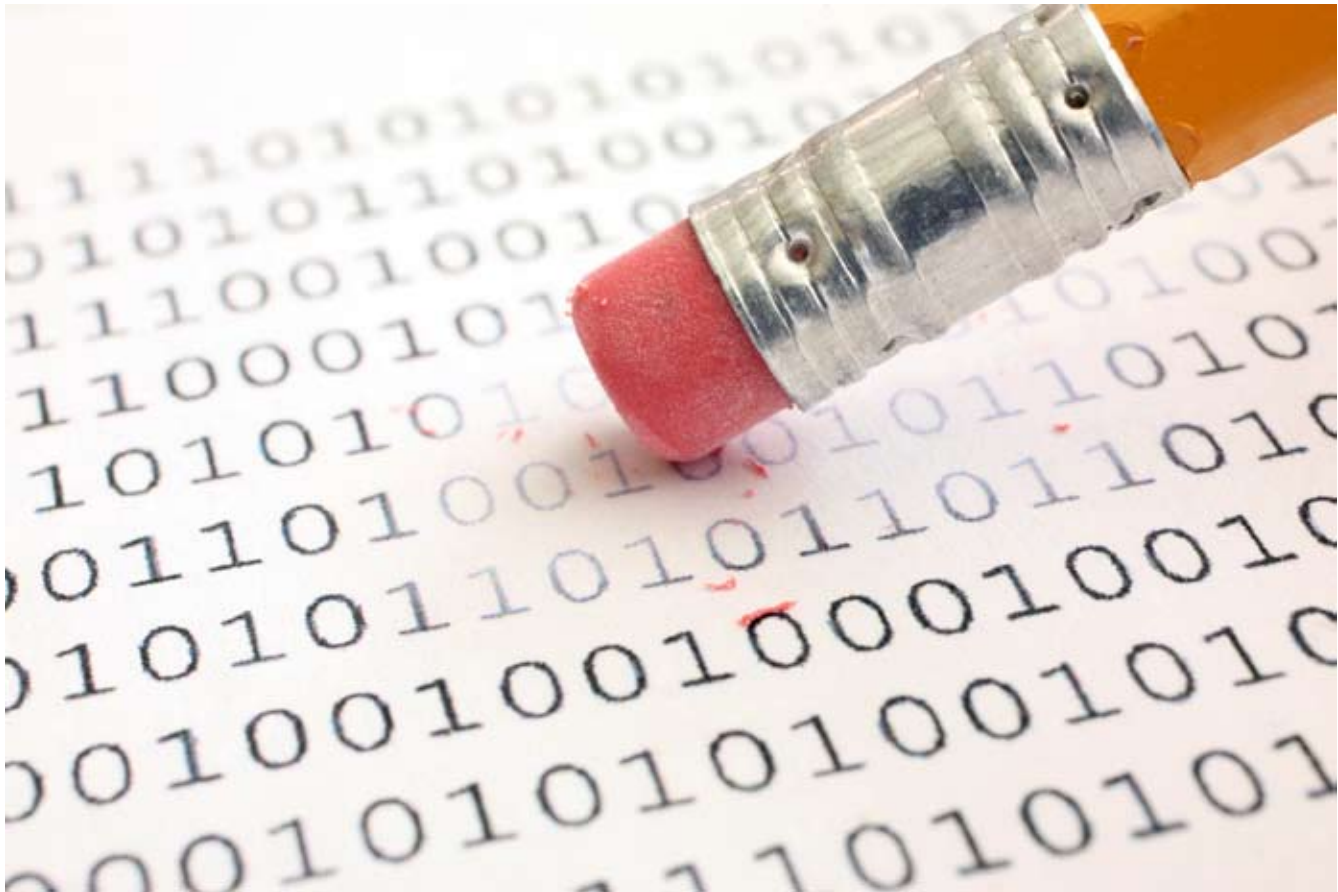
data is written to storage media, the more likely it is that the deleted data will be overwritten. Also, the longer storage media is used, the greater the probability of the deleted data being overwritten. For this reason, it is always best to begin the forensic process

“Until it is overwritten by other data, the data will continue to reside on the media. ”

as soon as possible, but at minimum, isolation of the device is recommended, since the frequency of use affects the successful recovery of deleted data.

PICKING UP THE SLACK

Another factor in determining where recoverable data resides is the disk sector, which is simply the segment on the disk where data resides. Staying with our book analogy, a sector is the page on which the data is written. Depending on the size of the file, it can be written across one or more sectors. When a file does not use an entire sector, the unused portion is called slack space.



Understanding slack space is important because fragments of the original data can be found here. Consider the following scenario: File A is written to the storage device and fills an entire sector. Then file A is deleted, which simply erases its entry in the file allocation table. File B is later written to the same sector, but it only uses the first half of the sector. Left in the last half of the sector (the slack space), is a fragment of the old, previously deleted file A. Because of slack space, an examiner may be able to recover portions of a file, even if the entire file cannot be recovered.

GOOD APPLICATION BEHAVIOR

The way an application works also affects the ability to recover a file, or versions of a file, from a storage device. While applications have their own mode of operation, many of them make use of temporary files, which may contain significant amounts of data or entire copies of information.

One example of an application that makes significant use of temporary files is Microsoft Word. While it may appear to the user that opening and editing a document is a simple process, Word actually opens or creates a minimum of four temporary files

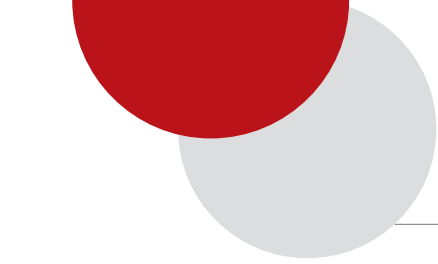
associated with that single document. At least one of these is a complete duplicate of the original file. When Word is closed, these temporary files are deleted (Microsoft Corporation 2007). Because of this behavior, numerous versions of a document can often be recovered from the storage media.

SCRUBBED (NOT SO) CLEAN

One common misconception is that formatting completely removes the data from the storage media. Instead, formatting only recreates the file allocation table and leaves the actual data on the media intact (Eckstrom 2007), meaning that data can be recovered from formatted media.

To effectively remove information from a drive, every data bit on a drive must be completely overwritten, a process commonly called “disk scrubbing.” Most scrubbing utilities will write a series of alternating 1’s, 0’s or random characters to the entire drive, ensuring that it cannot be easily recovered (Zetterson 2002).

However, even after using scrubbing utilities, it may still be possible to recover some data. According to Peter Gutmann, a well-known computer scientist from the University of Auckland, New Zealand, using anything less than 35 complete passes on a drive leaves behind “ghosts” (Zetterson 2002). These ghosts are created because of the proximity of the positive and negative



charges used when writing data to the drive (Gutmann 1996; Zetterson 2002). While this theory can be proven, actual recovery of data after scrubbing activities is more challenging. At this point, data recovery may still be possible, but it would require extremely advanced recovery methods.

One such advanced method involves the use of scanning tunneling microscopy. This process looks at the drive at the atomic level, detecting the change in density of the electrons at the disk surface. Scanning tunneling microscopy takes extreme amounts of time to find even small amounts of data and is only performed by highly skilled professionals (Zetterson 2002). Because of the significant costs and skills involved with this process, it is not usually practical to attempt this type of recovery.

PROVING THAT DELETED ISN'T GONE

So what can you really find using computer forensics? The short answer is just about anything. From 2002 to 2003, two students from the Massachusetts Institute of Technology purchased 158 used drives and discovered over 5,000 credit card numbers, medical information and other private data (Garfinkel & Shelat 2003).

This example is not an exceptional incident. A few years ago, as part of my preparation to become certified in computer forensics, I purchased a large quantity of used hard disk drives via eBay. Because they had been formatted in an attempt to delete their information, all of the drives initially appeared to contain no data. However, once the drives were examined using

specialized forensic software, numerous bits of information were recovered. Included in these recovered bits of data were family photos, a company's ordering database and another company's employee database. Within the recovered employee database were the addresses, phone numbers, Social Security numbers and work schedules of the employees.

ONCE LOST, NOW FOUND

Because computer forensics can be such a significant tool for strengthening a client's position, it helps to understand how it works. Comprehension can help the legal profession to better anticipate what to expect when utilizing a forensic examiner's skills. Additionally, this understanding also helps to interpret an examiner's findings and their report.

Beyond recovery of data, another benefit of computer forensics lies in the ability to prove data authenticity and provide details not found in typical metadata. As with any evidence, proof of authenticity can be vital to a case.

Of course, perhaps the greatest service computer forensics provides is in simply recovering data that was thought to be lost. Even though printed copies of documents have been destroyed, though the e-mail and its attached file has been deleted, though the backup tapes are found to be unreadable, computer forensics may often recover the data. And that's why deleted doesn't really mean gone. **ILTA**

RESOURCES

Eckstrom, P. R. "Holiday Edition: Why deleted isn't really deleted." Weblog Entry. Tech-for Everyone. 3 Sept. 2007. 8 Dec. 2007. <<http://techpaul.wordpress.com/2007/09/03/holiday-edition-why-deleted-isnt-really-deleted/>>

Garfinkel, S. L., and Shelat, A. (2003). "Remembrance of Data Passed: A Study of Disk Sanitization Practices." IEEE Security and Privacy , 01.1 (2003): 17-27.

Gutmann, P. Secure Deletion of Data from Magnetic and Solid-State Memory. July 1996. Dept. of Computer Science, University of Auckland. 8 Dec. 8 2007. <http://www.cs.auckland.ac.nz/~pgut001/pubs/secure_del.html>

Microsoft Help and Support. 6 June 2007. Microsoft Corporation. 15 Dec. 2007. <<http://support.microsoft.com/kb/211632>>

FAT32 File System Specification. 6 Dec. 2000.. Microsoft Corporation. 8 Dec. 2007. <<http://download.microsoft.com/download/1/6/1/161ba512-40e2-4cc9-843a-923143f3456c/fatgen103.doc>>

Zetterson, H. (2002). "Deleting Sensitive Information: Why Hitting Delete Isn't Enough." SANS Institute. 8 Dec. 2007. <http://www.sans.org/reading_room/whitepapers/privacy/691.php>

China and Sarbanes-Oxley

by Ashley Coover, MessageSolution

The global focus on enterprise compliance and electronic discovery efforts began in 2002 with the Sarbanes-Oxley Act (SOX), created in response to a variety of corporate scandals in the U.S. SOX has spawned similar legislation in countries around the world. Soon, all eyes will be on the People's Republic of China, a country that has been playing an increasingly important role in the global financial market.

This summer, China will begin enforcing regulatory standards similar to those of the SOX Act outlined in a seven-chapter piece of legislation called the Basic Standard for Enterprise Internal Control. Referred to informally as the "Chinese Sarbanes-Oxley Act" The Basic Standard for Enterprise Internal Control will regulate internal governance practices for all publicly traded enterprises located in mainland China, effective July 1, 2009.

China's Basic Standard for Enterprise Internal Control will bring stronger corporate governance to China's listed companies by addressing five control elements: internal environment, risk assessment, control activities, information and communication and internal monitoring. More than 800 enterprises listed on the Shenzhen Stock Exchange and more than 900 enterprises listed on the Shanghai Stock Exchange will be directly affected by this legislation.

One of the greatest challenges Chinese enterprises will face is responsibly managing their massive volumes of electronic information and corporate communications. The Basic Standard for Enterprise Internal Control will require Chinese enterprises to be able to capture, index and store electronic information contained in a variety of locations and formats in a secured yet easily accessible central location.

Along with retaining relevant corporate intelligence in the case of an audit or litigation, enterprises must be able to rapidly and thoroughly search through millions of e-mail messages and documents to retrieve information that could be critical for enterprises to pass audits, meet litigation challenges, avoid incurring penalties and retain stockholder trust. Many Chinese enterprises will turn to enterprise archiving solutions as the foundation for meeting these new requirements for internal policy management and transparency. **ILTA**

We're talking about litigation support online right now.

ILTA MEMBERS, join your peers online in the ILTA E-Group discussion forums. This popular member benefit is a members-only, topic-driven, online forum designed to improve communication among peers. There is no better place to get advice, exchange ideas, learn from first-hand experience and benefit from the knowledge of other legal IT professionals.

How does it work?

Log in to E-Groups from the ILTA homepage and subscribe the forums that interest you. New posts and replies will be sent to your e-mail inbox as often as you like. Post a message or reply of your own to get answers and recommendations from your peers.

Who can subscribe?

Any employee of a member law firm or law department can subscribe to any ILTA e-group.

TAKE THE CONVERSATION ONLINE



Don't miss out on one of the most important benefits of ILTA membership.

Disaster Recovery or Discovery Disaster?



The Drawbacks of Backup Preservation

INTRODUCTION

Rule 1 of the Federal Rules of Civil Procedure (FRCP), and of most state courts, aspires for the “inexpensive determination of every action.” Yet, as words like “gigabyte,” “terabyte” and “petabyte” enter the legal lexicon, the goal stated in Rule 1 seems farther and farther out of reach. The greatest burden in e-discovery lies in the ability to store electronic information in these ever-increasing quantities and at ever-decreasing costs. While recent amendments to the rules of civil procedure have attempted to rein in these costs and burdens, technological developments continually threaten what seem to be even the brightest of bright line rules. This article discusses the case for and against the inclusion of backup tape retention as part of a standard litigation preservation protocol, the current state of the law regarding the expectations and obligations of a litigant to preserve backup tapes, the challenges presented by even the most well-conceived backup tape preservation process, and claims about a next generation of search tools that may erase the current line between reasonably accessible and not reasonably accessible electronically stored information (ESI.)

Backup tapes, in particular, present many challenges to the goal of reducing the expense of litigation. The

identification and retention of extant, and in many cases, subsequent backup tapes is a common feature of preservation regimes in larger cases, if for no other reason than to serve as the last line of defense against a spoliation claim. This is true even when the parties do not expect that such backup tapes will ever serve as a source of discovery.¹ In this sense, backup tape preservation serves as a readily available and inexpensive form of insurance. For example, a 100-GB backup tape now costs well under \$100, and 1-TB backup tapes have recently hit the market. In addition to being relatively inexpensive, the tapes are extremely reliable and stable, and have a low per-tape operating cost. These, of course, are all the reasons why tape continues to serve as the media of choice for disaster-recovery backups of business systems, notwithstanding the emergence of equally voluminous disk-based systems. However, the prevalence and relatively low cost of backup tapes does not necessarily make them an appropriate or efficient means of preserving documents and data for litigation. Excessive reliance on backup tape preservation has the potential to create a false sense of security for a litigant. And unlike insurance, which ultimately requires only a small out-of-pocket deductible payment, the cost of having to resort to backup tapes to fill in gaps in active system discovery is significant. Backup tapes are a cheap form of insurance if you do not need it, and an extraordinarily expensive form of insurance if you do.

Consider too that if a litigant takes appropriate steps with regard to preservation in active systems and with key custodians, backup tapes will likely multiply in number and volume over the course of litigation. An attempt to preserve a discrete category of information through backup tapes will often require the preservation of significant quantities of irrelevant material and the data frequently will be redundant data that can be retrieved in more accessible formats and locations. In other words, backup tapes are, at best, a blunt instrument for litigation preservation. A company of any size that routinely retains backup tapes as a part of their normal litigation preservation protocol will soon be retaining backup tapes in perpetuity, as subsequent litigation, or the threat of litigation, attaches new preservation obligations on backup tapes retained in connection with a prior matter.

BACKUP PRESERVATION AS A MATTER OF HABIT

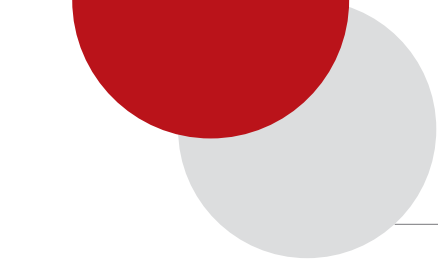
Recent amendments to the FRCP offer some reason to rethink the conventional wisdom that backup tape retention must be part of any meaningful litigation preservation regime. Rule 26(b)(2), for example, acknowledges that “[a] party need not provide discovery of electronically stored information from sources that the party identifies as not reasonably accessible because of undue burden or cost.” Similarly, Rule 37(e) instructs courts that “[a]bsent exceptional circumstances, a court may not impose sanctions under these rules on a party for failing to provide electronically stored information lost as a result of the routine, good-faith operation of an electronic information system.”¹² Admittedly, neither of these rules specifically mentions backup tapes, but they could qualify as a source that the party identifies as “not reasonably accessible because of undue burden or cost.” This is because of the costs and efforts involved in restoring, locating and producing ESI off backup tape. ESI is often overwritten due to the routine operations of a party’s IT system (such as the regularly scheduled recycling of backup tapes).

Other legal authorities have taken a much stronger position against the preservation of backup tapes in the ordinary course of a litigation hold. The Sedona Principles, perhaps the most widely regarded treatise on the topic, flatly recommend that “preservation obligations should not extend to disaster recovery backup tapes” absent exceptional circumstances (*The Sedona Principles: Best Practices, Recommendations & Principles for Addressing Electronic Document Discovery* cmt 5.h & ill. i (2d ed. 2007)). Among other reasons, the Sedona Principles observe that “employing proper preservation procedures with respect to the active system [such as a timely and periodically re-issued preservation notice

requiring affirmative acknowledgment of receipt and compliance by individual custodians] should render the preservation of backup tapes on a going forward basis redundant.” They then contrast this typically redundant nature of backup tapes with the misperception “that backup tapes are inexpensive and that preservation of tapes is not burdensome.” They also state that “because information on backup tapes is generally not retained for substantial periods of time, but instead is periodically overwritten when new backups are made, preserving information on backup tapes would require the time-consuming and costly process of altering backup systems, exchanging backup tapes, purchasing new tapes or hardware, and storing the tapes removed from rotation.” Concluding that “it is unreasonable to expect parties to take every conceivable step to preserve all potentially relevant electronically stored information,” the Sedona Principles advise that “[a] reasonable balance must be struck between (1) an organization’s duty to preserve relevant evidence, and (2) an organization’s need, in good faith, to continue operations.” Or, as the authors of the Sedona Principles have stated more recently in a July 2008 commentary, “[i]f the burdens and costs of preservation are disproportionate to the potential value of the source of data at issue, it is reasonable to decline preserve the source[;] . . . otherwise, transactional costs due to electronic discovery will overwhelm the ability to resolve disputes fairly in litigation.”¹³ (*The Sedona Conference Commentary On: Preservation, Management and Identification of Sources of Information that are Not Reasonably Accessible* 14 (July 2008)).

Courts, too, generally have adhered to the distinction between reasonably and not reasonably accessible ESI, placing backup tape data in the latter category and often relieving a party of the associated burden of backup tape preservation, as a result. The *Zubulake v. UBS Warburg*, 229 F.R.D. 422, 424 (S.D.N.Y. 2004) decision states, “As a general rule, [a] 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.” *Rowe Entertainment, Inc. v. The William Morris Agency, Inc.*, 205 F.R.D. 421, 431 (S.D.N.Y. 2002) further states that “[A] party that happens to retain vestigial data for no current business purposes, but only in the case of an emergency or simply because it has neglected to discard it, should not be put to the expense of producing it. In this case, the backup tapes clearly fall into this category.”

To be fair, it is not typically the case that ESI on backup tapes is literally not accessible (except where older tapes may have been preserved long after the legacy systems required to access them have been decommissioned), but rather it is prohibitively expensive, labor intensive and time-consuming to restore backup tapes in order to return ESI to a searchable format. Courts have tended to use an analysis that focuses less



on whether the litigant can afford it and more on the cost of accessing the ESI compared with its significance to the case. In *Wigington v. CB Richard Ellis, Inc.*, 229 F.R.D. 568, 572-73 (N.D. Ill. 2004), the court acknowledged that, even for a corporate litigant, “several hundred thousand dollars for one limited part of discovery is a substantial amount of actual dollars” and enough to make such discovery not reasonably accessible.⁴

WHY COURTS HAVE SANCTIONED PARTIES FOR FAILING TO PRESERVE BACKUP TAPES

So how does this claim that the retention of tape backup is neither an effective nor necessary component of a litigation preservation scheme square with the horror stories of litigation hold failures reported in the industry journals, advance sheets and e-mail alerts? Virtually every one of the decisions imposing sanctions on a litigant for “failure to preserve backup tapes” is really a case about the litigant’s failures to issue a timely and effective litigation hold to the key custodians within its control, to update and re-issue such notice as necessary, to monitor the effectiveness of the litigation hold during the course of the litigation, or to fully understand the operation of its IT system. In *ACORN v. County of Nassau*, 2009 U.S. Dist. LEXIS 19459 (E.D.N.Y. Mar. 9, 2009), the court decided the defendant’s failure to issue a prompt litigation hold, combined with the routine destruction of daily and weekly e-mail backups, supported imposition of spoliation sanctions. In *In re Intel Corp. Microprocessor Antitrust Litig.*, 2008 WL 2310288 (D. Del. June 4, 2008), the court questioned whether the defendant properly preserved evidence when it issued hold notices instructing employees to move relevant e-mail messages to separate media or their local hard drive, while allowing its automated e-mail purge to continue to run, and failed to preserve any backup tapes until four months after the filing of the complaint, particularly when the defendant either did not realize, or did not disclose, the operation of its purge function to the other side or the court.

If a “hide the ball” or “only if the other side clearly and undeniably asks for it” approach to discovery ever was an effective litigation strategy, it certainly has the potential to complicate matters in the event of a discovery dispute over an alleged failure to preserve ESI properly.

BACKUP TAPES NOT NECESSARILY OFF LIMITS

Technology stands still for no legal doctrine, and recent claims about a next generation of backup search tools may imperil the relatively short-lived but widely held view that ESI on disaster recovery backup tapes is not readily accessible and therefore not within the required scope of

discovery or preservation. These next-generation tools claim to be able to index, search and output files directly from a backup tape, without first having to restore the entire backup tape. Most of these next generation tools were not originally developed as litigation search tools; therefore, important questions remain about the robustness of the search, the effect on underlying metadata and compatibility with less-common business applications. However, many of these issues are likely to be resolved in time, and the result will be a substantial reduction in the cost and time of processing ESI on backup tapes.⁵ Does that, in turn, mean that backup tapes are soon to be within the scope of required discovery and preservation? Perhaps not.

The cost of accessing ESI also includes the cost of searching and producing the responsive, nonprivileged information retrieved from a backup tape. And, as any experienced practitioner knows, even the best-designed set of search terms flags far more documents than are truly responsive. The prevalence of such “false positives” can be a challenge when dealing with one gigabyte of active e-mail accounts, let alone the hits likely to be generated off a 100-GB backup tape. The federal rules, and many courts, suggest that such burdens can be reduced, for example, through sampling techniques; however, they offer little guidance as to the level of scientific rigor necessary to validate such sampling and perhaps overestimate the effectiveness of sampling as a cost reduction device.⁶ In *Citizens for Responsibility and Ethics in Washington v. Executive Office of the President*, 2008 WL 2932173 (D.D.C. July 29, 2008), for example, the court rejected the defendant’s objection to additional backup tape retention because the defendant “provide[d] no evidence, such as sampling or other statistical data, to support th[e] assertion” that “substantially all” of the relevant information already resided in more accessible location but failing to explain what kind of “sampling or other statistical data” defendant could or should have provided.

So the argument that ESI on backup tapes is not reasonably accessible is likely to remain, with simply a greater emphasis placed on the volume and cost of searching retrieved ESI. The ability to store electronic information is likely to continue to outstrip the ability to search and process it in a meaningful and cost-effective way; although, there will undoubtedly be an ongoing race between the growing capacity of storage media and improvements in the speed and efficacy of electronic indexing, searching and review tools.⁷

CONCLUSION

In summary, a litigant faces a range of obligations, options and considerations when crafting a litigation preservation strategy, particularly when deciding whether to make the retention of disaster recovery backup tapes a part of that process. Ample support exists in the rules of civil procedure, judicial opinions and other legal commentary to limit preservation measures to reasonably accessible, active systems only. Nonetheless, there is the understandable temptation to preserve an abundance of

backup tapes given the possible consequences flowing from a failure to preserve unique, material ESI. The preservation of backup tapes, however, should never serve as a substitute or remedy for the failure to issue timely litigation hold notices to key custodians, to monitor the effectiveness of these notices, to investigate and understand the IT systems at issue and to engage in the required disclosures and discussions with the other side about such issues. Moreover, if a decision is reached to preserve backup tapes, thought must be given to the: (1) volume of tapes likely to accumulate over time, (2) the cost of holding such backup tapes in the corporate storage management system or replacing them, (3) the potential disruption to normal business backup processes, and (4) the likelihood of being able to recycle such tapes given the prospect of future litigation. Any agreement to preserve backup tapes during litigation should be paired with a mechanism for periodically returning tapes to normal business backup purposes as the discovery progresses, even if this means going to the court to place such a provision in a document preservation order. **ILTA**

ENDNOTES

1. Iron Mountain, for example, reportedly has in excess of one billion backup tapes in its storage facilities.
2. But how safe is this safe harbor? The Advisory Committee Notes goes on to state that “[g]ood faith means that a party is not permitted to exploit the routine operation of an information system to thwart discovery obligations by allowing that operation to continue in order to destroy specific stored information that it is required to preserve. When a party is under a duty to preserve information because of pending . . . litigation, intervention in the routine operation of an information system is one aspect of what is often called a ‘litigation hold.’”
3. The Sedona Conference is not alone in expressing this view. The Conference of Chief Justices Guidelines for State Trial Courts Regarding Discovery of Electronically Stored Information § 9 (August 2006), for example, counsels that a preservation order, in general, “should be drawn as narrowly as possible to accomplish its purpose so as to limit the impact on the responding party’s operations” and “require balancing the danger to the electronically stored information against its materiality, the ability to maintain it, and the costs and burdens of doing so.” Similarly, in *Managing Discovery of Electronic Information: A Pocket Guide for Judges*, p. 18 (2007), the Federal Judicial Center advises judges that “preservation orders may, for example, exclude from preservation specified categories of documents or data whose cost of preservation substantially outweighs their relevance in the litigation, particularly if the information can be obtained from other sources. Moreover, as issues in the case are narrowed, the court should reduce the scope of the order.”
4. See also, e.g., *Aguilar v. Immigration & Customs Enforcement Div., Dep’t Homeland Security*, 2008 U.S. Dist. LEXIS 97018 (S.D.N.Y. Nov. 21, 2008) (relying on Sedona Conference Principles and Fed. R. Civ. P. 26(b) to conclude that restoring and searching e-mail backup tapes not justified where “the cost of this additional discovery is unquestionably high and the likely benefit low.”); *Young v. Pleasant Valley Sch. Dist.*, 2008 WL 2857912 at *2-3 (M.D. Pa. July 21, 2008) (declining to require production of material from backup tapes where, among other things, “[t]he material sought is most likely obtainable from another source that is more convenient, less burdensome, or less expensive” or at the very least is “simply cumulative”); *Petcou v. C.H. Robinson Worldwide, Inc.*, 2008 WL 542684 at *2 (N.D. Ga. Feb. 25, 2008) (concluding that cost and burden of restoring and searching e-mails on backup tapes would outweigh its likely benefit, and ordering defendant instead to retrieve undeleted e-mails held in the active e-mail account of an employee specifically identified by plaintiffs and any directly material undeleted e-mails from other employees of which defendant was aware).
5. Indeed, recently proposed amendments to the California Rules of Civil Procedure may portend such a paradigm shift by placing the burden on the responding party to assert the inaccessibility of ESI, seemingly suggesting a presumption that all ESI is accessible, unless a contrary showing can be made.
6. See Advisory Committee Note to Fed. R. Civ. P. 26(b)(2). First, sampling does not eliminate the need to restore backup tapes and de-duplicate or cull ESI from it. A quote of \$500 per backup tape restoration and \$150 per gigabyte of filtering would not be unprecedented, meaning an initial cost of \$15,500 per tape just to get the ESI from a single 100-GB tape to the point where attorney review could occur. Moreover, applying typical social science standards regarding sample size and levels of confidence, a universe of 100 such backup tapes would require a sample of 80 to yield a statistically significant result at a 95 percent confidence level with a confidence interval of +/- 5 percent. That translates into an initial outlay of over \$1,000,000 simply in backup tape restoration and processing costs.
7. Producing electronically filtered but otherwise unreviewed ESI under a clawback agreement could offer at least a partial solution to the burden of searching retrieved ESI, but it comes with its own drawbacks. Even with the promise of its return, most litigants are extremely wary of disclosing privileged documents, particularly sight unseen. Moreover, significant privacy concerns could be implicated with regard to such unreviewed production of ESI from servers that house personal data or e-mail accounts of employees, particularly employees in the EU. A fuller treatment of the pros and cons of a clawback arrangement are beyond the scope of this article.

Legal Hold and Subpoena Compliance Coordination



Many law firms struggle with how to effectively manage legal holds and subpoenas directed towards them. With the collaborative efforts of records, IT and litigation support, Morrison & Foerster (MoFo) has been able to devise a solution that is standardized yet flexible enough to deal with the many different scenarios that a law firm might face.

ASSESSING THE RISK

The first questions I'm asked when discussing our legal hold process are: What do you mean by legal holds and subpoenas? Isn't that what litigation support handles? At MoFo, litigation support is generally responsible for working with attorneys on active matters where one of our clients is involved in some kind of litigation. Typically, there are lots of client materials involved, and MoFo is handling the litigation process. The focus of this article, however, is on the "other" type of legal holds and subpoenas; those referencing a previous matter that our firm worked on. Most of these matters begin with our Risk Management Committee.

At MoFo, the coordination of this process is the responsibility of the records department, because the legal hold process has developed from our client transfer procedure, originating in the records department. This may seem strange, but records has traditionally been responsible for gathering all data, regardless of data type, for review and eventual transfer out of the firm. For MoFo, the legal hold process is very similar to client transfers. We need to know where the data lives, we need to have a process for gathering the data, and we need a way for attorneys to review the materials. These are the same steps our records department uses to manage client transfers. It does not necessarily have to be the records team that coordinates the compliance effort at your firm, but some group needs to be in charge of coordinating this effort. For MoFo, that's our records folks.

CONSISTENCY COUNTS

The benefits of having a designated group manage this process are twofold. First, it is important to have a consistent process. At our firm, we found that when attorneys coordinated the effort, the results varied. Secondly, it is also important for attorneys to be able to focus on the review of the materials and not waste time with the administrative tasks. Often these

matters are non-billable, so it makes sense to have attorneys focus on reviewing.

Consistency is the key to a successful process. You should have a process that is repeatable, and these steps should include:

- **Communication with the responsible attorney**
- **Notification**
- **Tracking compliance**
- **Gathering**
- **Reviewing**
- **Producing**

Communication — This is the most important step in the process. From the very beginning, the compliance coordinator needs to be working with the responsible attorney. There are some basic questions that need to be answered in order for the process to proceed smoothly. These include:

- **Is this a legal hold or subpoena** (i.e., are we just putting a hold on the data or is there also going to be a review)?
- **What is the scope?** Does this hold involve the entire client, or is it an individual matter?
- **How complex or extensive is it?** Does it involve five timekeepers or 50? Are we dealing with 10 folders or 100 boxes?

Each legal hold or subpoena is going to be different, and these types of questions will help you draft a clear and concise notification message.

Notification — Determine who needs to be notified and what instructions need to be given. At MoFo, all timekeepers and their secretaries are included on the notification e-mail message. Records uses a small .net application that allows us to gather all the names and hours of all the timekeepers that worked on the matter, and it also populates the cc line of the e-mail message with the secretary of each timekeeper. The body of the notification e-mail message has standard language describing the steps each timekeeper must take to comply with the legal hold or subpoena. Based on the information gathered from the responsible attorney, this language can be tailored.

Tracking Compliance — To be successful, you need to have a way to track that timekeepers have complied. At MoFo the notification e-mail message includes voting buttons such as the following:

- **No – I have no documents/e-mail**
- **Yes – I had documents/e-mail, and I have complied**

We also have a tracking spreadsheet on which we track everyone's response. We continue to remind timekeepers until we have received a response from them. Attorneys understand the importance of this process and do comply.

Gathering — As the timekeepers are complying, you can begin to start gathering the data. It is very important that you have constant communication with the responsible attorney so that everyone is on the same page. If you are dealing with a legal hold, you may only be placing a hold on the data. How firms place a hold will vary. You need to work with your Risk Management Committee to determine your firm's plan. At MoFo we do the following:

- **Relabel the folders in the Records Management System (RMS) to include a "DO NOT DESTROY" label**
- **Copy all documents in DM to a DVD**
- **Copy all documents in our shared drives to a DVD**
- **Store all e-mail messages in our RMS**

Our records department is not responsible for all of these tasks. As the compliance coordinator, however, our job is to make sure the appropriate department has accomplished its tasks and that we track the completion of this process. The DVDs are entered into our RMS and stored in the firm's safe.

Reviewing — Once everything has been gathered, you are now ready to make the data available to the attorneys. At MoFo we try to make this process as easy as possible for the reviewing attorneys. For example we pull all the gathered e-mail messages from the RMS and run them through a de-duping process, which normally reduces the number of messages by about 30 percent. We also separate the messages that came from or went to people outside the firm from those that are only internal messages. Once this is done, we place them in a public folder in Outlook. This allows the reviewers to view the messages through a format that is very familiar to them. Physical folders may be delivered, and documents are gathered for review.

Producing — The responsibility of determining what is to be produced is the job of the attorney. As the compliance coordinator, our department's job is to make sure all the data is available and that the process is moving forward. In many instances the team reviewing the data comprises associates and paralegals. Records staff stay in touch with them and ensure the review will meet the deadline date.

At MoFo we have learned that this process needs to be consistent yet flexible. We have a standard process and standard language; this allows us to be flexible when we need to be. It is also important to understand that any group responsible for this process (IT, records, litigation support) cannot succeed without the help of the other groups. Designing a compliance plan should always be a group effort. **ILTA**



Best Practices for Legal Hold Processes

In litigation, both organizations and individuals have legal obligations to identify, preserve, collect and ultimately produce information related to the matter under discovery. Unlike paper, electronically stored information (ESI) is more easily lost, modified, overwritten and deleted unless active steps are taken to manage this process throughout the life of the matter.

The source of many problems and sanctions encountered in litigation can often be traced back to some deficiency or oversight in the litigation hold process. What does or doesn't happen early in this process often has a greater impact on the costs of discovery and the eventual outcome than many people realize. Fortunately, many of these costs or adverse outcomes can be avoided by implementing and following best practices.

Despite all of the discussion and debate, the revised Federal Rules of Civil Procedure (FRCP), which were amended in December 2006 to explicitly address ESI-related issues, have not significantly changed the underlying nature of these legal obligations. While the revised FRCP have been a focal point for considering changes in discovery practices, the underlying obligations have been with us for quite some time.

Even beyond litigation, it's important to have appropriate processes in place for preserving information

in such matters as internal and government investigations. Due to the massive shift to storing all kinds of information in electronic formats, many have recognized the need to create and implement best practices to meet these obligations appropriately and to reduce associated risks and costs. Some, however, have learned the hard way that these are not obligations and processes to lightly disregard.

Crafting, adopting and implementing legal hold best practices often raises the following questions:

- **When is our legal obligation to preserve information triggered?**
- **Where is all of our data relating to this matter?**
- **How should we notify people of the need to preserve their information?**
- **Who needs to be notified?**
- **How much or how little information do we need to preserve?**
- **How can we best preserve and collect the data to meet our legal obligation?**
- **When should we rely upon custodian self-selection of data to preserve, and when is it more appropriate to follow a different procedure?**
- **When can we dispose of the information preserved subject to the legal hold?**

A CASE IN POINT

The recent court decision in *Keithley v. The Home Store.com, Inc.*, 2008 U.S. Dist. LEXIS 61741, 2008 WL 3833384 (N.D. Cal. August 12, 2008), is very instructive for establishing best practices on a number of levels. The underlying dispute involved an alleged intellectual property (IP) infringement of web site technology relating to the real estate market. Much of the discovery centered around the source code used. Unfortunately for the defendants, they made a number of mistakes leading to a costly set of monetary sanctions as well as an adverse inference jury instruction.

The duty to begin data preservation arose more than two years before the suit was even filed. The defendants had received a letter from the plaintiffs stating that “we assume that Homestore.com wishes to litigate this matter. Unless we hear otherwise by close of business Tuesday, August 7, 2001, we will advance this matter accordingly.” The court found this was sufficiently clear to inform the defendants that litigation was reasonably anticipated. The lawsuit was later filed on October 1, 2003.

While reasonable minds might differ on whether the defendants should have issued a legal hold and begun data preservation efforts upon receipt of the letter, certainly all would agree that the duty would have been triggered at the commencement of the lawsuit at the very latest. The defendants not only failed to recognize this, but they also did not meet their legal obligations during the next 16 months after the suit commenced. The court stated, “As it turned out upon further investigation, however, the question of how far in advance of the filing of the lawsuit the duty arose is largely academic, because Defendants did not satisfy their duty to preserve even after this lawsuit was filed and recklessly allowed the destruction of some relevant source code as late as 2004.”

The court explained why this case demonstrates the need for organizations to develop and follow a comprehensive litigation hold process: “The lack of a written document retention and litigation hold policy and procedures for its implementation, including timely reminders or even a single e-mail notice to relevant employees, exemplifies Defendants’ lackadaisical attitude with respect to discovery of these important documents.”

In the end, the court found that “[t]he discovery misconduct by Defendants in this case is among the most egregious this Court has seen,” and awarded \$320,000 in present sanctions, an adverse inference jury instruction impacting the scope and duration of the IP infringement, and also awarded future cost sanctions once Plaintiffs incurred and substantiated them.

While *Keithley* is an extreme example, it clearly underscores the need to establish and follow a well-thought-out legal hold process and supporting procedures.

Organizations looking to adopt best practices in their litigation readiness and response plans would be well advised to incorporate all of the following factors:

PLANNING

Understanding where and what types of data are involved, and taking the time well in advance to appropriately identify the resources needed to preserve and collect them, are key success elements in any legal hold plan. It will be far less costly and the process less error-prone if you address legal hold processes proactively. Conversely, mistakes and oversights are apt to occur when people are under the gun after a complaint or other triggering event crops up, especially while you and your preservation team are deep in the middle of other projects.

Also consider the level of expertise needed in your planning process. It’s important to have the relevant stakeholders involved from legal, IT, records, HR, compliance and other business units as appropriate. Sometimes cooperation across these departments can be strained due to culture, economics, conflicting priorities and other factors. Having an experienced eDiscovery consultant or outside counsel involved is often a key value add. Not only are you bringing in a wider range of expertise than what may be available in-house, but you gain the advantage of having a neutral facilitator who can more easily bring these important stakeholders together to develop an effective process.

TIMELINESS AND PRIORITIZATION

An effective legal hold process should include procedures for identifying when the obligation to preserve arises, whether it’s upon the commencement of a lawsuit or upon some other advance notice. Due to the transitory nature of some forms of ESI, it’s important to act quickly to prevent the destruction, modification or other loss of data due to normal operations and the action or inaction of others. It’s important to know where your data resides, the format or type of data, its retention cycle and the window of opportunity for collecting or preserving it within your acceptable levels of risk. It’s also important to prioritize your preservation efforts by identifying early on which data is at risk for spoliation, such as data that is being overwritten or expired daily.

USE THE MEET AND CONFER WISELY

While the duty to preserve is typically triggered before the FRCP Rule 26(f) Meet and Confer occurs, this conference should not be overlooked as a critical point for further scoping your preservation, collection and production responsibilities for that matter. With savvy advance preparation, the Meet and Confer is a powerful opportunity to limit the scope of discovery to more reasonable and cost-justified parameters. Courts are increasingly looking to the parties to proactively and meaningfully agree to their relative discovery responsibilities at the outset of the case.

Consider the recent federal appellate decision, *In re Fannie Mae Securities Litigation*, _ F.3d _, 2009 WL 21528, 2009 U.S. App. LEXIS 9 (D.C. App. Jan. 6, 2009). The attorney for a non-party, the Office of Federal Housing Enterprise Oversight (OFHEO), had agreed to a stipulated order during a hearing regarding his client's objections to discovery-related subpoenas. This trial counsel agreed to the restoration of backup tapes, searches using terms provided by another party, and production of the resulting non-privileged e-mail and attachments.

However, the attorney apparently didn't realize that, due to the scope of this agreed-upon discovery, he was ultimately committing the client to spend over six million dollars to comply. This amount represented over nine percent of the agency's annual budget, which was even more of a bitter pill considering that it wasn't even a party to the litigation. Nonetheless, the court insisted on the agency's compliance with its agreement and ultimately sanctioned the agency for failing to do so.

While this occurred in a hearing separate from the Meet and Confer, it serves as a strong warning for counsel to be fully advised and clearly understand all the ramifications of different approaches to eDiscovery before agreeing to them. Retaining eDiscovery experts and service providers early in the process to advise on such matters may well prevent commitments to uninformed and potentially disastrous timelines and search protocols.

COMMUNICATION, DOCUMENTATION AND AUDIT TRAIL

Effective data preservation is a team effort. Thus it's important to have clear lines of communication across the organization and with outside providers relating to roles, responsibilities, specific tasks, deadlines, and of course, the actual hold notifications. Unfortunately, it's not uncommon to hear "I didn't know," or "No one told me . . ." when problems arise. It's also not enough to simply issue the initial hold notices and hope that everyone will naturally comply. Courts are increasingly critical of passive or lackadaisical oversight of the legal hold process.

Many things need to be well documented so your organization is well prepared to withstand scrutiny. In the recent case of *Acorn v. Cty. Of Nassau*, 2009 WL 605859 (E.D.N.Y. Mar. 9, 2009), only a verbal hold was issued for a period of time. Along with other failures, this resulted in the court's finding that the defendant

Nassau County was grossly negligent in failing to implement a litigation hold and the court consequently imposed sanctions.

The lesson here is to document a wide range of items during the hold process. These include the forms and timing of hold notifications, the follow-up steps taken, by whom, when, and just as importantly, why. When deliberate decisions are made to not preserve data (when it is clearly duplicative) or collect data (when ESI is not reasonably accessible), it's equally important to document the reasons and justifications. An audit trail is necessary to help your organization or client keep track of both completed and outstanding tasks and will help provide sufficient evidence to rebut allegations of spoliation, negligence and other discovery failures.

ACCOUNTABILITY

The legal hold process is only as strong as the weakest link in the chain. Therefore, it's advisable to clearly identify each person's or group's responsibilities and the procedures

they should follow. It's also important to set up various checks and balances. For example, when there is an allegation of personal or corporate wrongdoing, it's usually not a sound idea to allow those involved to access or control the relevant data during preservation and collection activities. Your legal hold process should be able

to withstand scrutiny from opposing parties and the court.

CONSISTENCY AND REPEATABILITY

An effective legal hold program is one that relies upon defined processes and policies, and appropriate training for all those involved. These defined policies and procedures must also be followed consistently and repeatedly to be effective, and ultimately, defensible. Both litigants and judges will hold you accountable for following your own rules, assuming that your practices are not held to be unreasonable. Therefore, your organization also needs to develop a feedback mechanism and continuous improvement program to understand how well your processes and policies are being followed, and to identify areas where additional improvement may be needed.

IDENTIFICATION

Due to the transitory nature of ESI, organizations need to quickly identify sources of relevant information upon a triggering event to prevent spoliation. While many organizations have already developed an enterprise data map, it's also important to identify locations and data types at the custodian level. Without this information, it can take precious time for counsel and IT to understand on which shared drives

“An effective legal hold program is one that relies upon defined processes and policies, and appropriate training for all those involved.”

and servers a particular person has access and has stored data, as well as smartphones, hosted services including social networking sites, home computers and portable storage devices.

Also, a well-planned legal hold process includes the identification of potentially relevant departed employees and the correlation of their data against pending legal holds. Most organizations tend to quickly recycle a departed employee's computer, smartphone and portable storage devices; therefore, an exit checklist should be put in place that runs these data sources and their custodian's name against the list of employees subject to currently pending legal holds. It's fairly common to hear that custodians' hard drives were reformatted or re-imaged after they left the company, even though they may have been subject to a litigation hold. In the current economic environment of massive reductions in force and corporate restructuring, it is especially important that your process also incorporates methods for identifying and tracking the new custodians who "inherit" the data of their departed co-workers.

PLANNING FOR TRANSPARENCY

At some point, your internal processes and actions may be placed under scrutiny, and you may be asked to produce the records of your identification, preservation and collection processes and activities. Failure to do so may lead to a finding of negligence, monetary sanctions, adverse inference instructions and even terminating sanctions, such as dismissal or default judgment.

Transparency also needs to be anticipated in reference to tracked information. While this documentation needs to be accessible by your legal team, it's prudent to maintain it in a way that protects your various privileges, including attorney work product and attorney-client communication. Thus, while you may maintain lists of custodians, their ESI and the various statuses of each, be careful not to record or include potentially privileged information, such as attorney interview notes and legal impressions, in the same sources, lists or reports that may need to be produced to the court or opposing counsel. It may prove helpful to exercise control by segregating the factual from the privileged information. This way, you can produce information about the steps taken to meet your legal obligations without disclosing privileged legal strategies.

INFORMATION LIFECYCLE MANAGEMENT, INCLUDING EXPIRATION

With the paradigm shift to storing most information as ESI, many organizations have found it challenging to develop or simplify their records retention programs. In many instances, records management schedules

designed for paper documents haven't transitioned well to managing electronic files, necessitating the need to radically simplify and reduce the number of relative retention and expiration categories. Also, depending on the hold strategies employed, everyday users are often being tasked to manage their own data both before and during legal holds, with greatly varying results. This presents increased risk in the legal hold process.

E-mail messages are typically of high interest in many types of litigation and investigatory matters. Absent a legal requirement to retain it, organizations need to balance the business value derived from retaining e-mail against the legal risk and costs of doing so. Having more e-mail, attachments and related data at hand can require additional work, time and cost to identify, collect, cull, search, review and produce, even with automated tools. In addition, over-retention can create serious implications for the efficient operation of electronic systems and the costs of increased data storage. It's important, therefore, to look beyond the legal hold in managing costs. Considering that document review is often the largest cost of discovery (comprising as much as 70 or 80 percent), the less data there is for review, the lower the resulting costs.

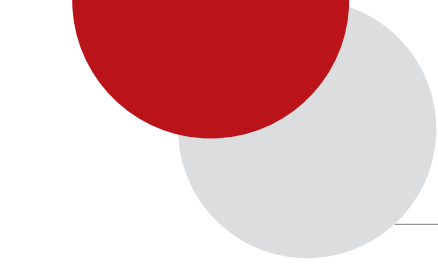
Some organizations have already turned to e-mail archiving as a part of the solution. However, some care is needed in determining what should be archived, and how. Some archiving vendors may recommend archiving everything into a central archive or vault, but that could have the unintended effect of "moving the landfill." Also, implementing an archive system that does not provide sufficient eDiscovery-related tools, such as robust searching, culling, reporting and exporting, could very well result in more time-consuming and costly efforts to get the relevant data back out of the e-mail repository.

Suffice it to say, when adopting best practices for legal holds, it's critical to assess the organization's overall information management policies, practices, and tools, as they can have a profound impact on the effectiveness, risks, and costs of eDiscovery and other business processes.

SUPPORTING TECHNOLOGY AND AUTOMATION

As seen in numerous eDiscovery cases, mistakes sometimes occur from miscommunication, disorganization and human error. With reductions in the workforce, there is often a loss of key organizational knowledge, sometimes referred to as "institutional memory." In many situations, there are simply fewer people with less time to devote to these tasks. However, when lapses in the process occur, the risk of spoliation and resulting sanctions can rise dramatically.

The proper application of supporting technology can often automate and increase consistency in the legal hold process while reducing risk and cost. Organizations commonly rely upon e-mail for distributing the initial and ongoing hold notifications and subsequent tracking with spreadsheets. People



are already familiar with these tools, and they can easily be produced with technology that the organization already owns. But also consider the enhanced benefits of implementing dedicated legal hold tools. Rather than relying upon human intervention to manually review e-mail responses and spreadsheet entries, consider a system that automatically alerts you to nonresponders and automatically sets reminders for follow-up. This has the added benefit of providing constant “real-time” information, rather than having to wait for someone to update it manually.

Also consider that unless spreadsheet cells are protected, there is always the risk of a user inadvertently deleting or changing tracked information in a way that renders it inaccurate. Short of keeping prior file versions, spreadsheets do not contain an audit trail capability regarding cell content changes. Another common mistake, which increases risk, is when a person inadvertently overlooks custodians or data sources contained in other worksheet tabs or other off-screen content. By the time this overlooked information is discovered, if at all, extensive spoliation can have occurred.

Consider, too, that storing legal hold spreadsheets on a network or local drive makes it more difficult for multiple people to access or update the information. Local drives should definitely be avoided due to general lack of regular backups and risk of loss. In contrast, legal hold systems are typically database driven and may allow varying degrees of concurrent access depending on the user’s security profile. By recording events as they are logged, legal hold systems also generate logs or audit trails, a critical element when the process comes under scrutiny.

THE GIFT THAT KEEPS ON GIVING

The legal hold process is a critical stage in eDiscovery. Implementing and executing a well-designed legal hold process can significantly reduce the risks and costs associated with eDiscovery. Implementing these best practices should be viewed as a critical investment. With discovery sanctions easily reaching into the millions of dollars and beyond, avoiding one or a handful of legal hold mistakes could help recoup this investment. Beyond this, creating and executing an effective legal hold process built upon best practices results in significant efficiency-driven cost savings year after year. **ILTA**

TEN LEGAL HOLD BEST PRACTICE TIPS:

1. Take the steps to identify in advance where potentially relevant data is stored in active systems, backups, archival systems and other locations, such as portable devices and third-party hosted systems.
2. Put in place methods to identify, as early as possible, those who should be contacted for the timely preservation of data potentially related to the matter at hand (individual employee/custodians, enterprise and business unit data custodians, IT, third parties and collection service providers).
3. Confer with outside counsel and service providers early in the process and throughout to set clear goals and expectations to reduce risk.
4. Prioritize your hold efforts to address relevant evidence most at risk for spoliation if quick action is not taken to preserve it.
5. Develop written hold notice templates as appropriate, and retain copies of sent notices. They may be needed when your legal hold process is challenged.
6. Identify which temporal ranges (date ranges) will be needed for the legal hold, including ongoing preservation requirements.
7. Develop exit checklists and processes for reviewing departing employees’ legal hold obligations. These should identify and inventory their data sources, such as laptop hard drives, portable storage devices and smartphones, and relate both the departing custodians’ name and their data to existing hold matters. In addition, identify their successor data owners. Coordinate with HR as appropriate.
8. Incorporate personal follow-ups with individual and enterprise data custodians as part of your legal hold process. This is often a critical and effective step to learn more about the data, nature and merits of the case. Document and track each follow-up, keeping in mind the need to preserve privilege.
9. Differentiate between those matters where custodial self-selection is advisable and those that are not (*e.g.*, fraud, employment, and various types of investigations). Plan for implementing forensic and other collection methods to reduce the risk of spoliation and foul play in particularly sensitive matters.
10. Manage your data before it manages you and your budget.

The Premier Educational and Networking Event in Legal IT

ilta09

Leading technology | optimizing value

ILTA's Annual Educational Conference for 2009, **Leading Technology | Optimizing Value**, is where decision-makers will share their experiences, as technology leaders to explore innovative technologies and collaborate on how to best optimize the value of IT in law firms and law departments, a particularly important focus in departments. In our current economic climate, the ability to participate in such a variety of offerings at one conference truly maximizes the value of attendance!

This **four and a half day event**, featuring educational content across **26 tracks**, is universally regarded as THE place to further your professional development, learn from your peers and make valuable connections. **If you are only able to attend one conference this year, ILTA '09 will provide the best value to you and to your firm.** The combination of applied peer practices, in-depth technical knowledge and executive business content promise to provide an outstanding educational lineup for leaders at all levels of your organization.

Among the 192 sessions are topics of particular interest to litigation support professionals:

- Interactive Session on Advanced Trial and War Room Set-Up
- Future of Our Profession: What Lies Ahead?
- When Is Full-Blown Forensics Necessary?
- eDiscovery Reconnaissance: - Early Case Assessment Cracks the Code
- Controlling Litigation Support Costs: Strategies for Cost Control and Recovery
- How to Structure Your Litigation/Practice Support Department
- From Good to Great: LitSup Providers Become Expertise Ambassadors
- Litigation Support Technology as a Value Foundation for Clients
- Can You Recover Your IT and Litigation Support Costs?
- The Impact Litigation Support Has On Your Network
- Litigation Support Roundtable Discussions

August 23 - 27

**Gaylord National
Resort & Convention Center
Near Washington DC**



twitter.com/ilta09

visit <http://conference.iltanet.org> for more information

The Effects of Litigation Holds on the Corporate Lawyer

Conceptually, a litigation hold is a request issued to direct employees to retain any information relevant to an event or potential topic of dispute. In practice, there are several challenges that can impact the success of a hold, including the ability of recipients to conform to the hold in theory or in practice. The instructions as issued in the *Zubulake V* decision require attorneys to take “all necessary steps” to ensure litigation holds are followed. That direction makes it necessary for attorneys to, at the very least, have a familiarity with the information technology and human resource policies and procedures that relate to the preservation of information.

To the attorney, a litigation hold conveys the communication to a person in a business department that an obligation exists to retain information related to a topic or event. The topic of the hold can be described simply and is generally understood by the recipient because it involves their department, and they are usually familiar with it. However, confusion can occur when the recipient of a hold begins to read and interpret the definition of what information is covered by the hold and, if included, what they should do to preserve it.

There is a significant difference between the legal definition of a “document” and the records management meaning of a “business record.” Attorneys can define “document” to have a variety of meanings, and their explanation can be an example of confusing legal words resulting in an unclear definition. A records and information management (RIM) policy can be so precise and controlled that it does not provide any leeway to extend the attributes of a relevant document to allow it to become a business record. With an absence of clear direction, the result will likely be an unsuccessful litigation hold. There are steps attorneys can take, however, to address these challenges and ensure a more successful process.

STEP 1: DEVELOP AN EFFECTIVE LITIGATION HOLD FORM

The challenge in establishing a template or form for a litigation hold is that, by their nature, templates and forms usually lack the qualities that ensure a meeting of the minds with their recipients. Unless the obligations that a hold requires can be communicated in a clear, legalese-free manner, the success of the hold can be jeopardized. Rather than following a legal template or form, litigation holds that go into the business departments should have the personality of business documents. A successful litigation hold template takes a substantial commitment by the lawyer to develop, update and issue the hold.

The following are suggestions for developing an effective form:

- **Offer what direction you can.** Attorneys need to issue holds quickly, sometimes before there is a problem they can easily define. That lack of knowledge can hinder their ability to establish rapport with the recipient of a hold. Follow-up communication and other holds will be necessary as the substance of the matter unfolds.
- **Speak Clearly.** Address the who, what, where, when and how of the hold in business unit language and terms. A litigation hold requires that activity happen immediately. By clearly communicating what needs to happen within a time frame that is almost always “now,” the recipient can prioritize the hold actions to address them at once.
- **Lead with, and highlight, the action items.** Rearrange the format of the hold to place a description of what needs to happen first. The legal language can follow once a person clearly understands that the hold is for them and that they must act.
- **Minimize content.** Attach technological instructions and reference materials rather than pasting them into the body of the litigation hold. Recipients who need technical assistance can schedule a time and place to address the specific instructions.

- **Offer assistance.** Include contact names and numbers for recipients to ask questions. These contacts should include the attorney issuing the hold, an IT person who is familiar with the structure and methodology of the hold procedures, and a records management contact for questions about how the materials for the litigation hold should be treated in the RIM process.
- **Follow-up.** In addition to reminders that a hold remains in effect, letting the recipients know that you will be in communication with them as part of their case investigation, lets them know what will follow the hold.

Clearly the time and effort to establish teams to respond to inquiries, develop documents across functional areas and obtain a consensus of the content within a legal department is considerable.

STEP 2: ADDRESS THE TECHNOLOGICAL CHALLENGES

Despite all direction to the contrary, a certain number of recipients will promptly forward e-mail messages and send files to the attorney issuing the hold. Others will give all their attention to meticulously organizing their e-mail without a thought to the loose files they have stored on their computer. E-mail and Microsoft Office files are usually the focus of hold activities for both attorneys and recipients. However, there can be a variety of file types that business units manage, and a comprehensive litigation hold will result in the retention of all of them.

Adding to the complexity of a litigation hold is the fact that it is rare for a company to have only one hold in place at a given time. If there are overlapping hold topics or events, there can be more confusion about how to save files that pertain to multiple holds that may have separate time frames. Superseding or amending a litigation hold can perplex the recipient as well. Once expanded topics, the method for organizing files, and instructions on how to copy or move files to alternate locations are introduced in a litigation hold, recipients can be further confused. Since attorneys are responsible for ensuring the hold compliance, it is no small task to ensure that recipients understand what they are to do when a hold is originally received or modified.

A significant source of frustration for attorneys and employees is the ability to preserve electronic information. Attorneys may instruct employees to retain data, but in the course of doing so, they may need to modify IT policy and intervene for the recipients to ensure the hold can be followed. Attorneys who issue litigation holds are required to understand the procedure for storing files and enforce that plan with

the business departments when conflicts arise. In companies where storage space and e-mail database size is metered to employees, a litigation hold will require special instructions. Each employee receiving a hold must be instructed on where to place files, how to organize them and who to contact for more space if needed. It is imperative that storage space allocations be in line with IT policy for a long term solution. Additionally, personal storage options are typically small and inexpensive, and hold recipients may be tempted to use a hard drive, flash drive or out-of-the-way network area to store their files. The goal of a hold is not only to retain the files, but also to retain them in a reliable method.

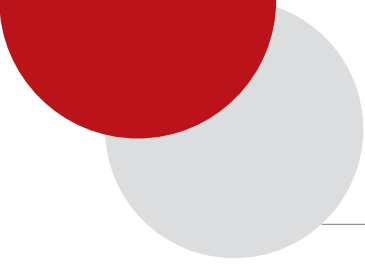
STEP 3: COMMUNICATE AND FOLLOW-UP WITH APPROPRIATE DEPARTMENTS

Along with the obligation to retain relevant information, the business units are usually required to bear the expense of the litigation holds. The legal department needs to participate in the business decisions to ensure that adequate procedures and cost allocations are in place to adapt to the scope of litigation holds. From an IT perspective, business files are data, while the legal mind focuses on the content of those files. A litigation hold does not mean data is preserved “somewhere” on an ad hoc basis. The attorneys are required to ensure that decisions are made in advance of the holds to be successful. Employees are usually at the mercy of management decisions and IT scheduling of backups, upgrades and technology refreshes. Litigation hold recipients can have the best intentions to follow a litigation hold, and still, the measures they take may be inadequate and incorrect. While every attorney does not need to be an IT professional, it is imperative that they follow up on the holds to ensure that the proper information is stored in the proper locations.

The litigation hold is the worst enemy of the managed storage budget. The perception is that storage is cheap. While storage devices may be less expensive than they once were, managed storage is a business expense that considers more than the wholesale cost of the space. Attorneys need to arm themselves with enough knowledge to understand the impact of the litigation hold they issue. This can be in the form of an IT resource who is knowledgeable about the file locations and IT policies of the company, communicates with the legal department to define the scope of the obligations and can buffer the discussions about the budget. Knowing that IT departments focus on data placement or storage, rather than content and meaning, it should come as no surprise to learn that sometimes when attorneys research the locations of relevant data, they find that data has been purged.

STEP 4: BUILD RELATIONSHIPS WITH THE PEOPLE WHO HANDLE THE DATA

In addition to the business departments that hold the subject matter of a litigation hold, attorneys must invest in grooming



relations and communications with the human resource departments. There are many activities that impact the location of data that is applicable to a litigation hold. Attorneys have to ensure that every deactivated user, such as an employee moving to a new location, transfers his or her data to a custodian who is held accountable for it. Attorneys are required to lead the campaign against purging data without research and evaluation; promote the idea that business units and administration have the obligation to give the preservation of information the

priority it requires; and help different departments understand that sometimes rules don't apply.

"All necessary steps" to ensure litigation holds are followed is an open-ended phrase that has a significant impact on the law department and its attorneys. The detour that attorneys are required to take around the practice of law can be significant. Every discussion an attorney has with anyone in the company during the investigation of a case should begin and end with a confirmation that they understand and are following the litigation hold issued to them. **ILTA**

Tips and Tricks for Creating a Search Term List

by Janet M. Hornsby, IE Discovery, Inc.

Creating a search term list can be a daunting task even when you're familiar with your document collection. It doesn't matter whether it is a list to search for relevant documents, privileged documents or something more unique, refining your search terms to locate that "smoking gun" isn't easy. Try these ideas to boost your confidence in the outcome of your next search:

- Build plenty of time into your discovery plan to allow for creating your list, reviewing the results, refining the terms and running the list again. Most people underestimate the time that will be required to create an accurate search term list.
- Find someone who is familiar with the documents in your collection to assist you. Someone that has used a particular form that you want to locate might know that the name of the form changed over time. You can then add or change terms to find that version.
- Be sure and allow for variations of terms and acronyms to ensure that you are not missing documents. When searching for names, include aliases, nicknames and e-mail addresses; and allow for possible typographical errors and misspellings.
- Make sure you understand how to write terms correctly for your particular software. It won't matter how well you choose your terms if the incorrect wildcard is used. If you are unsure of the outcome, seek out a programmer or other expert to assist you.
- Avoid overly broad terms, especially when the document collection was done in a sweeping manner.
- Run test searches of your individual terms before running the entire list. If you can discover that a term is too broad or too specific in the beginning of the task, you can save yourself a good deal of time in the long run.
- Don't be afraid to refine your terms. Try variations until you have just the right balance to find what you need without pulling up unnecessary documents. However, make adjustments for the right reasons! Make sure you are changing search terms to actually respond to a request or to be more exact in finding the right information, not simply to reduce costs or to avoid producing certain documents.
- Don't just look at the false positives, but also look at the remainder of your collection for misdetections. It is as important to know what you missed as knowing what you found.
- Document, Document, Document! As you make changes to your list, keep records of each change and why it was made so that you have the information to defend your decision, if needed. **ILTA**

FTI TECHNOLOGY

YOU ARE ABLE TO **COMPLY** WITH A MASSIVE
ESI PRODUCTION REQUEST. ON TIME. ON BUDGET.

BE READY.
BE RIGHT.SM

YOU MOVE FORWARD WITH CONFIDENCE
THAT THERE WILL BE **NO SURPRISES.**

Get on top of critical e-discovery challenges and get the outcomes you're after with FTI TECHNOLOGY.

Hundreds of cases in various stages of e-discovery. Pending litigation. Regulatory inquiries. Internal investigations. No matter what your e-discovery challenge, *be ready* with FTI TECHNOLOGY. Ready with a solution tailored to your unique business needs. Ready with a global team of experts to help you at any stage of e-discovery. Ready with proven software to reduce, review and produce critical data in any format. Be ready, so you can *be right* with your e-discovery results. FTI TECHNOLOGY. **Be Ready. Be Right.**

Visit ftitechnology.com/control for the free industry analyst white paper:
"Getting Control of Electronic Discovery: How In-House Technology Delivers Savings"
or call 206.373.6565 for more information.



Ringtail™ Attenex™

©2009 FTI Consulting, Inc. All rights reserved.

ABOUT THE AUTHORS

JEFF BEARD is a senior consultant in Daticon EED's national eDiscovery consulting practice. Jeff uniquely bridges the legal and technological circles by drawing on his considerable experience with law department operations and supporting technologies including both legal and enterprise systems. He is a frequent national author and presenter. His popular blog, LawTech Guru (www.lawtechguru.com), regularly covers new developments in eDiscovery. He can be reached at jbeard@daticon-eed.com.

MICHAEL IWAN is a partner in the Minneapolis office of Dorsey & Whitney LLP. He is a member of the firm's Labor & Employment, E-Discovery, Class Action, and Appellate practice groups. He has extensive experience defending class action and collective action employment litigation and in complex e-discovery, preservation and forensic issues that arise in such settings. He also has spoken before various attorney and litigation support audiences on the practical and legal implications of e-discovery. He can be reached at iwan.michael@dorsey.com.

CINDY MACBEAN, litigation support manager for General Motors Corporation legal staff, oversees the Legal Document Processing Center and Global Product Development Information Center. Cindy is certified in eDiscovery as well as other litigation support programs in addition to holding an MBA in Technology Management. She has spent the majority of her career in law firms, first as a paralegal, then as a litigation support manager, where she developed, implemented and supported litigation support technology in a variety of specialties. She can be reached at cindy.macbean@gm.com.

TOM MORRISSEY is senior director, IT litigation at Purdue Pharma LP. Tom has worked in the litigation area for over 20 years and is the former manager of practice systems for Summation Legal Technologies, Inc. and CaseVault. Prior to that, he was the manager of practice systems at Kelley Drye & Warren. He is a past president of the National Association of Litigation Support Managers (NALSM) and East Coast Association of Litigation Support Managers (ECALSM). Tom can be reached at tom.morrissey@pharma.com.

DISCLAIMER This report is designed for use as a general guide and is not intended to serve as a recommendation or to replace the advice of experienced professionals. If expert assistance is desired, the services of a competent professional should be sought. Neither ILTA nor any author or contributor shall have liability for any person's reliance on the content of or any errors or omissions in this publication.

COPYRIGHT NOTICE Copyright © ILTA 2009. All rights reserved. Printed in the United States of America. No part of this report may be reproduced in any manner or medium whatsoever without the prior written permission of ILTA. Published by ILTA. c/o Editor, 9701 Brodie Lane, Suite 200, Austin, Texas 78748

CHRIS PAVAN is a co-founder 42 LLC. He started his career in the U.S. Army as an Electronic Warfare Technician, and has over 13 years experience in Information Technology & Security. For the last six years Chris has conducted numerous forensic examinations in civil, criminal, and government matters, and volunteers his time as a subject matter expert for various Southern California law enforcement agencies. He can be reached at chris@42llc.net

NICK RINGOLD is a consultant and expert witness in the field of computer forensics and electronic discovery. He has provided testimony and consultation in criminal and civil matters on topics as varied as data authenticity to discovery scope for multinational corporations. With over 15 years of computer technology experience, his work in this field began at the Sacramento Valley Hi-Tech Crimes Task Force and eventually progressed to Guidance Software, before co-founding 42 LLC. He can be reached at nick@42llc.net.

MIKE SINNWELL is currently the director of information technology at Belin Lamson McCormick Zumbach Flynn, a Des Moines, Iowa based law firm. Along with other duties, he conducts forensic examinations of electronic evidence. He also advises attorneys on information related to electronic evidence and electronic discovery. He has worked at the Belin Law Firm since November of 2005. His certifications include: CCE, CISSP, CISM, MCSE 2003/NT4, CNE, CCNA, Security+. Mike can be reached at msinnwell@belinlaw.com.

CHARLENE WACENSKE has been with Morrison & Foerster LLP since 2000. She is currently the firm wide records manager and the IT senior administrative systems manager. Working closely with IT, the records department rolled out a firm wide e-mail filing solution, which has resulted in over 15 million messages electronically filed in the firm's records management system. Charlene is past president of the Golden Gate Chapter of ARMA and is currently the Vice President for ILTA's Records Peer Group. She can be reached at cwacenske@mofo.com.

This publication is printed on 65# Mohawk 50/10 Cover and 60# Sterling Ultra Text that is FSC certified and is 10 percent post-consumer content. The inks are walnut oil-based and completely recyclable:



Think Green — pass this issue
to a colleague