

Where Is Your Data Located?

Meeting the Challenge of E-Discovery Across the Enterprise



Robert Childress and Jason Park

This hypothetical case study involving theft of trade secrets discusses data identification and collection issues to be considered and questions to be answered to ensure an effective e-discovery response.

Your company recently hired a hot shot from a competing company. The new hire seems to be a bright, promising individual with a ton of experience and connections. Everything seems to be going well until her former employer files a lawsuit alleging theft of trade secrets.

You, the director of records management, are brought into a conference room with your company's legal department and the former employer's outside lawyers. They instruct you to implement a litigation hold immediately. Now what?

Collaboration Required

Some of the initial considerations should be to assist the legal team in determining the scope of the data that needs to be placed under litigation

hold. The legal team will most likely have already made a number of decisions related to the scope of the records to be preserved since they will be familiar with the issues and the legal strategies that will be employed to provide defenses in the case. This includes relevant time frames for the records being preserved, the record types – maybe even in relation to the data retention policy – as well as relevant custodians.

The legal department's role should be to clarify what types of records will be necessary for their particular strategy. But, because the attorneys may not have an in-depth knowledge of the company's records, it is important for records management personnel to be involved. (See sidebar on page 55 for record-related issues to consider before

implementing a litigation hold.)

Decisions made at early stages of discovery may have ramifications later. Effective dialogue between records management and the legal team should address the pros and cons of the methodology that will be employed when rolling out the litigation hold.

Data Identification and Collection Methods

Once the initial legal strategy and preservation scope are determined, it's time to assess what data exists, how it's currently stored, and what methods of securing a legally defensible and forensically sound copy of the data should be employed.

Following are four steps organizations can follow to ensure they are con-

sidering all relevant sources of data and appropriate collection methods for each.

Step 1. Identify the pool of potential people whose data needs to be preserved.

The legal team should help you with this identification process, as should the preservation letter from the other side. This may include named parties, supervisors, supervisors' supervisors, and so on.

In this hypothetical case, the potential "custodians" are Suzie Salesperson (who came from the competitor), Billy Boss (who hired Suzie), and Tony Topguy (Billy's boss).

Step 2. Determine what equipment the parties who were identified above have been issued by the company.

Is there a record of the equipment placement in their human resources file, or is there an asset tracking program in use? If so, double-check to ensure all devices have been accounted for.

In this hypothetical case, Suzie, Billy, and Tony each have a company-issued desktop PC, USB thumb drive, and a BlackBerry.

Step 3. Identify what network resources the parties above have access to, whether users are required to authenticate themselves, if different resources require permissions to access them, and so on.

In this hypothetical case, Suzie, Billy, and Tony each has:

1. Workstation PC
2. BlackBerry
3. E-mail account
4. USB thumb drive
5. Group access to "sales" folder on Windows file server
6. Virtual private network access from home computer
7. Ability to send and receive faxes via desktop faxing
8. Voicemail
9. Voice over Internet protocol allowing for call forwarding

Issues to Consider Before Implementing a Litigation Hold

The Preservation Request

A preservation request is a document the opposing party provides near the beginning of a lawsuit to notify the other side that it needs to preserve certain data. Often, these requests are generic in substance, having been simply churned out using a template. Other times they are crafted very precisely.

If your job is to create and implement a litigation hold, it is crucial you view a copy of the opponent's preservation request and discuss what you have been requested to preserve and how to accomplish the task.

In some instances, the preservation requests may include verbiage similar to the following: "You are ordered to preserve active files, deleted files, file slack, and unallocated space ..." If you see this verbiage, a forensically sound bitstream image (like a DD image, a bit-by-bit image of a source device or file) will be required.

If the phrase "as kept or maintained in the regular course of business" or a similar phrase has been used in the preservation letter, there are issues to consider when collecting, processing, and producing the data.

When collecting data for preservation, file names should be preserved, but that is not all. If not collected properly, data can be altered, which means it will no longer be in the same state as it would have been kept in the regular course of business. This can happen by:

- Not maintaining folder structure, for example, by picking out selective files and dumping them all into a new folder
- Altering what is known as the MAC-Times (Modified time and date, Accessed time and date, Created time and date) for example by dragging and dropping or copying and pasting files

There are many other ways data can be altered during the preservation process. These alterations should be avoided or, at a minimum, they should be documented with an explanation.

The Data Retention Policy

Is your data retention policy always followed? How does this data retention policy affect your task of implementing a litigation hold on the data that's necessary to preserve? Do backup tapes need to be pulled from rotation and secured? Do devices like workstations, BlackBerry smartphones, and other mobile devices need to be cloned prior to redeployment to new hires?

The Meet and Confer Conference

A meet and confer conference is required under the 2006 revision of the *U.S. Federal Rules of Civil Procedure*. The idea behind the meet and confer conference is for the attorneys from each side of the litigation to disclose potential locations of electronically stored information and specify the format of the data. For the legal team to be thoroughly prepared prior to the conference, a complete assessment of the IT infrastructure (in-house and hosted) needs to be conducted.

10. Access to a web-hosted sales force customer relationship management application

Step 4. Decide which method of preservation to employ for each of the 10 data sources mentioned above.

Make decisions about how to collect data from each of the data sources. Be aware of repercussions that may be faced, depending on the choices that are made.

1. Workstation PC

Does this litigation hold require a complete bit-for-bit forensic copy of the hard drive, which copies deleted files, file slack (blank space between files on the hard drive), and unallocated space? Or will a ghost image, which copies only the active files, be adequate?

Pros: A bit-for-bit forensic copy is able to recover deleted files should they become important later in the litigation process. If the forensic copy has been made correctly, write-blocking techniques will have been employed, which help defend against alteration of the data at the time the copy was made. Write-blockers allow a one-way transfer of data out of the device to be copied, thus eliminating allegations of co-mingling or alteration of the data during the copying process.

Cons: Since the deleted files and unallocated space is preserved, attorneys may be forced to deal with this type of data. The attorney cannot argue, “If I don’t know about it, I don’t have to deal with it.”

2. BlackBerry

BlackBerry smartphones have their own set of issues. The data can be extended beyond the device, and knowing how each user interacts with his or her BlackBerry (or other mobile device) is helpful.

BlackBerry data can be acquired off the device utilizing a variety of mobile forensic software packages. Users can make backups of their BlackBerry smartphones utilizing BlackBerry

If the forensic copy has been made correctly, write-blocking techniques will have been employed, which help defend against alteration of the data at the time the copy was made.

Desktop Software, for example. This method results in files with the extension *.ipd, which can be rich in information if the *.ipd files are parsed. E-mails, call logs, text messages, among others, can be recovered from *.ipd files.

Who hosts the BlackBerry server? Does your company host it, or does the cell phone provider host it? If your company does, do you also have to preserve the BlackBerry server? If the cell phone provider does, should you notify it to preserve the data in the account in question as part of your litigation hold?

3. E-mail account

How do users access their e-mails?

If by WebAccess, are the login details logged? Are e-mails sent and received utilizing the WebAccess option replicated in the server?

If by POP via Mail Client, are the e-mails cleared off the server once the mail is stored in the client?

If by IMAP via Mail Client, are sent and received messages, as well as deletions, logged?

If users are able to create and backup online or offline mailstores (*.pst/ *.ost), interviewing them to determine if they do this and what method they employ will help identify other potential sources of data.

In this case, Suzie, Billy, and Tony have PSTs and OSTs on their local machines. E-mails exist in active format on the exchange server and older e-mails that meet the litigation hold criteria also exist on backup tapes.

What do you do to de-duplicate these mailstores so only one copy of the e-mails is added to the litigation hold? Luckily, there are a couple of options for this. Whichever tool is chosen, it needs to have the ability to de-duplicate the e-mails against the total population of e-mails on a per custodian basis, keep track of the original location of the e-mail, and keep track of the output location (regenerating a single new PST that contains unique e-mails, while maintaining the foldering system used by the user).

This is critical since the phrase, “As kept in the regular course of business,” was used in the legal documents coming from the other side, and it’s your duty to preserve or replicate this foldering system because the placement of the e-mails in sub-folders shows intent on the part of the user or custodian.

4. USB thumb drive

Does this litigation hold require a complete bit-for-bit forensic copy of the thumb drive, which copies deleted files, file slack, and unallocated space?

5. Group access to “sales” folder on Windows file server

Network shares present their own set of challenges. If the “as kept in the regular course of business” phrase is taken seriously, you need to ensure NTFS permissions, file system metadata, especially modified/accessed/created dates and times, as well as the folder structure created by the users, are all captured and preserved.

As records managers are often part of the team making decisions regarding methodology that will be employed when rolling out the litigation hold, remember all of the different areas data can live across the enterprise.

Remember, the attorneys want to know, “Who knew what, and when.” Some companies allow custodians to self collect their data, setting up a folder into which the custodians place relevant files. This methodology can face numerous legal challenges because the files are being removed from the place they were kept in the regular course of business and as such, the data structure is substantially different from where the data was kept on the server.

Dragging and dropping files is not recommended as a defensible file copy methodology. Robocopy (providing the correct switches are used and documented) can be employed, but it is probably advisable to use a tool that is specifically designed for this, since such tools will maintain the correct chain of custody documentation and logs.

6. Virtual private network access from home computer

Do the custodians have the ability to log into the work network from their home computers? If so, are the home computers company-issued machines designed to be used for telecommuting? If so, those machines should be acquired, too. If they were not company issued, and they were used for job functions, your organization may be facing a very tough decision.

Since the company was aware the users’ home computers were used to

access company information and the users chose to access that data from their personal home computers, an affirmative decision to potentially commingle company data with personal data may result in the employees’ home computers becoming discoverable, and, therefore, part of the litigation hold.

7. Ability to send and receive faxes via desktop

Some organizations have established desktop faxing. This allows users to send and receive faxes from their workstations without having to have the actual hard copy of a document.

Faxing programs convert digital files into TIFF images for the fax transmission. These images are not key word searchable without additional optical character recognition (OCR). This process should include the legal team, since they will be more familiar with the issues and the legal strategies that will be employed to provide defenses in the case being performed. If desktop faxing is employed (or other methods of scanning paper documents, for that matter), those files will have to be identified and additional OCR processing may need to be performed to make them key word searchable.

8. Voicemail

Does your organization provide

unified messaging which saves and forwards voicemail to individuals’ e-mail inboxes as an audio attachment? If so, those voicemail files may become discoverable.

9. Voice over Internet protocol for call forwarding

Does your organization allow for call forwarding of incoming business calls from the company phone lines to a mobile device? If so, how are voicemails left for the mobile device and the call logs saved to the device going to be handled? Are they discoverable? If an iPhone is the mobile device being utilized, the voicemail is actually saved on the hard drive of the phone itself, not on the carrier’s voicemail server.

10. Access to a web-hosted sales force customer relationship management application

Does your company outsource any part of its IT infrastructure and application maintenance? The most common functions outsourced involve payroll, accounting, and customer relationship management applications and services. Litigation holds may extend to data that is hosted by other entities on your behalf.

Collaboration Is Key

As records managers are often part of the team making decisions regarding methodology that will be employed when rolling out the litigation hold, remember all of the different areas data can live across the enterprise. Keep the dialog fresh between legal, IT, and records management because decisions made in any part of the process may have future ramifications. You will want to be able to say, “Here is the plan,” rather than have to ask, “Now what?” **END**

Robert Childress can be reached at robert.childress@discoverthewave.com. Jason Park can be contacted at park@md5group.com. See their bios on page 62.