

## LEGAL TECH

### Proven Methods to Prevent Spoliation of Online Data

By Jim McGann

In an article written by Beth S. Rose and Charles J. Falletta that appeared in the May 17 *New Jersey Law Journal*, the authors summarized the mistakes for which Judge Shira A. Scheindlin penalized The Pension Committee of the University of Montreal Pension Plan. The ruling focused largely on the improper preservation and collection of documents and data. Perhaps if the committee had taken an alternate approach to how they were preserving and collecting data, they could have avoided the sanctions.

Preservation or hold notices are common practice when attempting to secure electronically stored information (ESI) that may be potential evidence in a case. In order to prevent ESI spoliation, the legal team may issue a letter specifying that files and e-mail should not be destroyed and should be preserved in a reasonable manner. The objective of this preservation notice is to ensure that data not be modified, deleted or changed in any manner. As the data is still on the live networks, e-mail server or even a user's desktop, modification of the data is a likely possibility, especially for those who know where the "smoking gun" is buried.

*McGann is the Vice President of Information Discovery at Index Engines in Holmdel,*

Spoliation of data is always possible when dealing with online content that users still have access to.

This article will discuss new methods that are available to avoid spoliation of online data. New tools are available to collect data that represents a "point in time snapshot" of the corporate network and e-mail server. This "snapshot" is a forensically sound and incorruptible copy of data that can be called upon when spoliation or, as was the case with the pension committee, under-collection is a concern.

#### Risk of Spoliation

Preventing spoliation presents an attorney with a challenging task. By the time users, who have access to the e-mail and files in question, receive the hold notification, the data could easily have been changed. In day-to-day business operations, accessing many files and e-mail is common. At the simplest level a user could inadvertently change the access time of a file by viewing it, or a pertinent e-mail could be forwarded on to another user or even deleted before the preservation notice hits his or her desk. There are also situations where a document in question is under constant revision, such as a spreadsheet. If the case involves the content of this spreadsheet on a specific date, how do you go back to this date to ensure you have the accurate data?

Online data is sensitive and dynamic. Metadata can be easily changed, content can be modified, files and e-mail can be deleted. By the time the preservation notice is delivered, data spoliation can occur accidentally, or purposefully. There are no guarantees that the data in question will remain unspoliated, even when a hold notice has been issued. If a case depends on the accuracy of online data that is accessible by anyone on the corporate network, a better method of preservation must be employed.

#### Corporate Data Preservation

So how do you ensure that ESI is secure and accurately reflects the time in question? Before exploring the solution, let's review current corporate data back-up procedures and technology.

The IT department backs up corporate data from the network onto back-up tapes daily. In the case of a catastrophic failure, or even user error, specific files and e-mail can be restored from the back-up environment. Therefore, every file created or edited and every e-mail written is copied to a secure, typically offsite location for safe keeping. These backups represent "point-in-time snapshots" of the files and e-mail on the network and servers. So the e-mail in a custodian's inbox on June 30 or a contract created by a specific user, including revisions of this file, has an identical copy backed up by IT every day.

The ESI that is backed up to tape is secure and unspoliated. Users do not have access to this data. It cannot be modified and is a 100 percent accurate representation of what existed on a specific date.

Consider it a time capsule that can be called upon as needed. In order to be confident that no spoliation has occurred, instead of requesting data from the online network, legal teams should be issuing requests for data that was backed up to tape on the dates in question. No preservation letter is needed; the data is already preserved by the IT department during routine backups. Access to this data is easy, it is all collected and exists on tapes that are typically stored in a vault either onsite or offsite. Additionally, the request for this data is far less invasive as it will not require access to live corporate networks for the collection.

#### **Leveraging Existing Backups for Legal Hold**

Since secure, preserved data exists on offline back-up tapes, why are legal teams still issuing preservationers for easily corruptible online data? Because, previously, back-up tape data wasn't easy to access. As a result, legal teams have been forced to work with the more accessible data that exists online.

New technology now makes data on

offline back-up tapes accessible. Data that is locked away by IT during the routine back-up process previously required specialized skills and great expense to access. The tapes are generated using proprietary software that collects the data and places it into a back-up container that is copied onto tape. This process has required this software to gain access to the content. This is why in the past it was expensive and time consuming to gain access to files and e-mail on old back-up tapes. However, this is no longer the case.

This data is now easily available using new automated tape discovery tools. When ESI is required, simply request the appropriate back-up tapes from the client. These tapes are typically dated, so it is not difficult to find the relevant tapes for a specific timeframe. The tapes are then automatically scanned and indexed, so that they are searchable. Legal teams can then specify the specific metadata and content they require. For example, if you require a specific custodian's mailbox, or a copy of a contract from June 2000, or even a general search of specific mailboxes to

look for sensitive keywords, all data is now easily accessible via simple query terms. The relevant e-mails and files can then be extracted from tapes quickly and economically without any spoliation. The original back-up software is not required; in fact it does not require any specialized technical resources to get the job done.

As a result of this new approach, legal teams can now be confident they have the data they need to support or defend against a law suit, and be sure that it is accurate, as it is a snapshot of the content as it existed on the date required. Anyone who wants to tamper with or influence the outcome of a case no longer has access to potential evidence. This new approach toward ESI preservation is far more accurate and secure than the traditional method. No longer do you need to issue a preservation letter — just ask your clients for their tapes. They are already preserving what you need. Not only does this new approach eliminate the risk of spoliation, but the worries about under-collecting electronic data are now mute. ■