



DIGITAL DISCOVERY & E-EVIDENCE



VOL. 10, NO. 16

REPORT

SEPTEMBER 16, 2010

Reproduced with permission from Digital Discovery & e-Evidence, 10 DDEE 333, 9/16/2010. Copyright © 2010 by The Bureau of National Affairs, Inc. (800-372-1033) <http://www.bna.com>

BNA INSIGHT

Huron Consulting Group's Jake Frazier suggests some techniques for dealing with SharePoint, a source of ESI that has critical data, often has murky custodianship, is growing exponentially, contains intermingled structured and unstructured data, and is not maintained centrally or searchable across all locations.

SharePoint: The E-Discovery Blind Spot?



BY JAKE FRAZIER, J.D., M.B.A.

Jake Frazier, J.D., M.B.A. is a Managing Director at Huron Consulting Group and specializes in assisting corporations with in-house E-discovery and information Governance initiatives. Mr. Frazier can be contacted at jfrazier@huronconsultinggroup.com.

Just when you thought it was safe to go back into the water. . .

At the dawn of e-discovery, organizations first had to find some way to be able to identify, preserve, collect, and eventually produce relevant e-mail. In fighting that good fight they were likely knocked sideways when they then had to account for massive amounts of PSTs (or NSFs) on desktops. Once they nailed down some process to handle e-mail, they may have moved on to

file shares. Here is where the curve balls of finding even more PSTs, large I.T. dumping grounds of PC data, and the concept of files with no custodian or an owner of “admin” reared its ugly head. It’s likely that many organizations are still stuck at this point, in a drive to establish defensible and repeatable processes for the least amount of money.

Nevertheless, the next level of complicated e-discovery is upon us: SharePoint.

This complexity yields conversations in meetings preparing for an e-discovery matter that go something like this:

Consultant: “Let’s move on to SharePoint, how many sites do you have?”

I.T. Representative #1: “Last count, 17,000.”

I.T. Representative #2: “You’re forgetting about the acquisition; it’s more like 30,000.”

Legal Representative: “Our interview process should alert us to any SharePoint content we need and the key custodians have been asked to preserve any relevant information, so I think we are okay regarding SharePoint.”

There are several potential pitfalls with this approach that will be discussed below.

What’s SharePoint? For the non-technician, understanding SharePoint is challenging, but not impossible. A SharePoint site is essentially a website, usually internal, where multiple people can collaborate —loosely called a “team site” or “collaborative environment.” If you’ve ever tried to jointly publish a document with five co-workers and been caught in version-control nightmares with so many e-mails flying around with drafts in various stages of review then you are familiar with one of the problems SharePoint solves, and solves well. With SharePoint, that same document could have been uploaded, then routed to the correct reviewers, in order, and protected such that only the correct reviewer had access before moving the document to the next stage of the process— all while staying off e-mail. This is loosely called “Workflow.”

Key Terms. In dealing with I.T. on SharePoint, understand a few terms is key. The first is “MOSS.”

While SharePoint is really the application you see and log in to (the application layer), there are more systems underneath that make it all work. MOSS stands for Microsoft Office SharePoint Server (it is actually now called just Microsoft SharePoint Server, but the term MOSS still is widely used). Just think of this as the “guts” of SharePoint, and know it when you hear it.

The other term or terms have to do with “Web 2.0 collaboration.” In essence these terms refer to the wikis and blogs that can be created and used in SharePoint. These sites are key because many collection techniques rely solely on the documents that are loaded into or created in SharePoint (think Word documents) and not the wikis or blogs. Other than a few nuances like these, SharePoint needs to be considered another source of ESI that must be dealt with.

An Example. For example, imagine you work for a medical device designer and manufacturer. The collaborative nature of SharePoint can drastically improve the efficiency of many teams within the company. Perhaps most importantly, the research and development teams for a planned device can collaborate virtually with much more ease than trying to use e-mail or rely solely on live interaction, even on web conferencing.

Test results can be uploaded and searched, design specs can be routed to the proper person even amongst large teams, etc.

The Challenges. However, think of the ramifications. This means every single planned product, launched or not, has a SharePoint site containing a wealth of critical information related to each product. In any lawsuit regarding disputed ownership of product designs or product liability, for example, there is a SharePoint site simmering with relevant information. Strict reliance on a custodian model could be problematic in that alot of this data, such as the documents, wikis, and blogs in the site, don’t really belong to one custodian; by nature they are a by product of a collaboration between many.

Also, if a key collaborator is **no longer with the company**, the problem gets worse as there is no interview process to alert the would-be evidence collector to their presence, and no “self-selection” process for a key custodian to perform.

Another reason relying solely on a custodian model with custodian interviews to completely cover SharePoint as a source of ESI is problematic is the sheer volume and growth of SharePoint. For example, very large companies reported adding 109¹ SharePoint sites each month in a recent survey, with 24.7² percent of existing SharePoint sites dormant or inactive.

Some Comfort. The good news here is that legal and I.T.’s interests align. Just as we saw with e-mail archiving software providing dual benefits of: a) storage savings to I.T. and b) “searchability” and governance controls to Legal, the same type of solution is emerging for SharePoint. There are two sets of tools that, along with the right process and expertise, can help remediate the problems in relatively short order. The initial hurdle, however, is that Legal needs to be aware of SharePoint as a current blind spot, and partner with its I.T. counterparts and outside experts to begin understanding and solving the problem.

Identifying inactive sites and archiving the content to a repository that applies a retention period is now possible with the right combination of people, process, and technology.

SharePoint Governance and Archiving. With help from consultants, organizations can now create policies that can be enforced regarding the creation and archiving of SharePoint sites. If more than 25 percent of SharePoint sites are running but nobody is using them, then in essence the organization is maintaining a pond in which some future fisherman will be able to fish. Identifying inactive sites and archiving the content to a repository that applies a retention period is now possible with the right combination of people, process, and technology.

¹ “Gathering MOSS? Revealing SharePoint Opportunities and Costs,” InfoTrends, August 2009

² Ibid.

In addition, these tools offer I.T. a bonus return on investment, as they can be used to optimize the way SharePoint stores data—much like stubbing or short cutting of large e-mail attachments to slightly slower but cheaper storage helps I.T. reduce storage and backup costs.

Also, while SharePoint is often considered “free,” the source of the ease in which setting up new SharePoint sites began, MOSS is not free and I.T. is often interested in seeing how it can reduce license costs. These solutions are ideal for a joint return on investment for both Legal and I.T, and are ripe for conducting assessments in short order.

SharePoint E-Discovery. For organizations not yet ready to implement an information governance solution for SharePoint, there are tools that can reactively perform diligent identification, preservation, and collection from SharePoint. These tools could either be installed

and stay resident behind the firewall, or be used by consultants who are engaged to perform collections for the organization.

Typical “forensics” does not apply in some ways to SharePoint due to how the data is stored, but utilizing a forensically sound method is paramount, and use of tools that ensure no metadata is lost is a requirement. Be cautious; although there are many tools that interact with SharePoint, many were designed for something else, knowledge management for example, and while they may be marketed to conduct e-discovery on SharePoint, they fall short of the forensically sound standard.

Whether the initiated organization is ready for a complete information governance solution for the SharePoint phenomena, or needs immediate help in conducting e-discovery in its SharePoint environments, the right expertise and toolset now exist to help. Understanding that SharePoint may be the e-discovery blind spot is the first step.