

## Oh the stories a copier can tell!

By Richard E. Wills

**May 28, 2010**

In my February post *Getting The Geeks To Reboot*, I discussed changing an IT staff's perspective on how IT policies may have an effect on your company's exposure should you be required to execute a Litigation Hold or produce ESI as a result of a litigation. I was feeling pretty good about the work I had done to get my own house in order by examining backup retention policies, making data maps, and trying to think outside the box on how far our data might sprawl. Heck, I even figured out a way to reduce the life of digital dictation files on our system when they were finished being transcribed. I had it in the bag, or so I thought.

That was until I saw a recent *CBS Evening News* report regarding the security of digital copiers and scanners. It seems that most every copy machine manufactured since 2002 contains and uses hard disk drives. Better yet, most all of these copiers are now digital MFPs (MultiFunction Products) that scan, email, fax, and copy. As you'll see in the *CBS* report, the device has to store a copy of the document being printed or imaged on that hard drive in order to do its work. Worse, those images can be retrieved, in many cases, just as files on a computer hard drive can be retrieved. Think about that for a minute. Over the lifetime of a MFP device, millions of pages of documents have been scanned, copied, faxed, or printed. Hence, the same millions of pages of images have been stored on the hard drive at one time. While every page of every image may not be able to be recovered, these hard drives still present us with a treasure trove of ESI that could potentially be asked for in the discovery process.

While there is no case law that currently addresses ESI stored on copy machine hard drives, it seems like it's just a matter of time before it is addressed. So I made a few phone calls to my MFP vendors to determine what my options were. There were two issues that I wanted to address. The first being the removal of the ESI when our lease expires; the second issue was what, if anything, could I do throughout my lease to purge the images on a regular schedule. Something that I could create a retention policy for, configure my copiers to erase the data, and do so on a schedule dictated by the policy.

It turns out that my current equipment has no options for erasing the data on a regular schedule. The software that runs the copier was not designed to have that option; however, on newer models one can purchase the ability to do so. The option is very low in cost and something that I will include when the time comes to refresh my fleet of copiers. My vendors also have a policy in place that provides for a deep format of the disk drives upon the end of a lease using software that is DOD, NASA, and NSA compliant in order to destroy all data on the hard drives. At my option and for a cost, I can have the hard drives removed from the copiers before they leave my premises and take control of them in order to dispose of them myself. Since we utilize a service that physically shreds hard drives from our retired computers, spare hard drives, and servers, this seems to be the most secure way to dispose of the drives. Something to keep in mind as we adopt new technology and new devices is the storage that those devices use to do their work, how we manage them, and how we dispose of them. While the geek in me loves the fact that just about everything uses computer technology, sometimes the thought sort of wears me out.