

How to Deal with the Legal “Catch 22” of Electronic Data Destruction

By Dan Bayha

How does an organization comply with the two legal requirements mandating the destruction of obsolete sensitive personal data *and* the termination of data destruction during litigation?

Most large organizations have litigation going on almost on a continuous basis. Sarbanes-Oxley requires that all normal data destruction procedures be terminated once litigation begins or is anticipated to begin. Failure to comply with “legal hold” on all relevant data is considered a criminal activity, whether intentional or not.

Now both Federal and State legislation aimed at protecting individual financial and medical information requires any organization dealing with this type of information to destroy the recorded data prior to disposal. You must maintain written policies and procedures dealing with this destruction and have documented evidence of actually following the procedures on a regular and timely basis.

Plaintiff’s lawyers are constantly pushing the records-retention envelope as it relates to litigation discovery. It is not uncommon for legal proceedings to spend more time on document and data discovery issues than on the case’s substantive issues. Under these conditions, it is essential that an organization adopts and practices a record-retention and destruction policy that is reasonable and in good faith. A good record retention program can represent a legal “Safe Harbor” from plaintiff’s lawyers’ unreasonable data discovery demands.

The “Sedona Principles” (www.sedonaconference.org) is an attempt by the legal profession to establish a guideline for lawyers, records management, and information technology professionals for best practices in managing information records. These principles are becoming the recognized records-management rules that courts are relying on to determine proper legal discovery compliance.

A fundamentally important element of the Sedona Principles asserts, “Systematic deletion of electronic information is not synonymous with evidence spoliation.”¹ Proper destruction of electronic records or of other information consistent with a reasonable approach to managing information and records is not synonymous with spoliation of evidence or obstruction of justice. In the absence of extraordinary circumstances, if an organization has implemented a clearly defined records management program specifying what information and records should be kept for legal, financial, operational, or knowledge-value reasons, and has appropriate retention systems and/or periods, then information not meeting these retention guidelines can and should be destroyed.

A fundamental legal problem can and will arise if poor housekeeping of erased media is allowed. If erased media is identified within the discovery process, plaintiff’s lawyers have successfully argued that substantive information may have been erased. The appearance of a cover-up is more damaging, in fact, than the actual information that was erased.

Another major legal problem can arise from failure to dispose of old electronic media on a timely basis. Morgan Stanley recently lost a billion-dollar lawsuit on the basis of old back-up tapes being found in storage after the trial’s discovery process was closed. A common and costly occurrence is finding old hard drives with data still recorded and no documentation as to where they came from or what information is stored on them.

Your legal department will insist that forensic procedures be used to determine what data is on the hard drives prior to their approval to discard. This can cost tens of thousands of dollars.

Legal issues dealing with data destruction are significant. Historic disposal processes need to be reevaluated in light of increased liabilities. Data destruction methods require analysis to determine what method best protects your organization and meets with new regulatory requirements. Any changes should be reviewed and approved by legal counsel.

The following is an overview of destruction methods available today and highlights of the advantages and disadvantages associated with each kind of procedure.

A fundamental legal problem can and will arise if poor housekeeping of erased media is allowed. If erased media is identified within the discovery process, plaintiff’s lawyers have successfully argued that substantive information may have been erased. The appearance of a cover-up is more damaging, in fact, than the actual information that was erased.

Available Electronic Data Destruction Tools

Software Erasure Programs

Software erasure programs are the most commonly used tools in the private sector. These programs do not actually erase the data, but record over it. The more times you record over the data, the more secure the

process. The principal advantage of this tool is that it can be performed on-site and under management control. The erased media is usually reusable.

There are several problems associated with this procedure.

1. Defective hard drives cannot be erased.
2. It is a very time-consuming process; a large-capacity hard drive can take more than a day to erase, and the time required is constantly getting longer.
3. The use of software erasure tools on electronic media leaves evidence that erasure has occurred, which may possibly cause a legal discovery problem.
4. The process is mind-numbing and subject to human error.
5. Advancements in data recovery technology constantly challenge the effectiveness of software erasure tools and require constant and expensive software upgrades.
6. There is no way to easily visually check that the erasure has successfully occurred.
7. The media can be re-used but generally is technologically obsolete, leaving you with a physical device that must be disposed of.

Degaussing Equipment

Degaussing equipment is commonly used in the federal government and is the preferred NSA and DOD tool. These devices apply a strong magnetic field to tapes and hard drives and effectively destroy all magnetically recorded data. The NSA publishes the necessary magnetic field strengths to destroy data on different types of magnetic media and also a list of approved devices to use. The process is typically done on one storage device at a time and takes approximately a minute per device to perform. This is generally a significant time savings versus software erasure techniques. Degaussing equipment is located on-site, and data destruction occurs under management control. Certain types of tape media can be reused after degaussing.

There are several problems associated with this procedure.

1. Different types of magnetic media require different strength magnetic fields to properly erase. Unshielded reel tapes and older cartridges require relatively weak magnetic fields (600 Oe) and thus inexpensive degaussers can be used. New high capacity tape cartridges such as super DLT and DDS cartridges require much higher (2500 Oe) magnetic fields and much more expensive equipment. Degaussers must be matched to the type of media to be degaussed and the magnetic field of the degausser needs to be tested at least every six months.
2. The equipment is specialized. Operators must be trained in order to achieve the desired results. Degaussers only work on magnetically encoded media. Optically encoded media is unaffected.
3. Degaussers generate strong magnetic fields. Any sensitive electronic device, such as a heart pacemaker, or stored magnetic media needs to be shielded.
4. Magnetic fields dissipate quickly over distance; thus degaussing fields are physically small and require one-at-a-time hand feeding. Powerful degaussers utilize shielded chambers that are very limited in size. Some larger server hard drives are too large for the chamber. All mounting brackets and "hot swap" caddies must be removed prior to degaussing.
5. There is no way to easily visually check that the degaussing has successfully occurred. The only test is to remount the media and try to read it.
6. Magnetic media that uses manufacturer prerecorded header information is damaged and can no longer be re-used. You are left with a physical device that must be disposed of.



Figure 1: Combining in-house software erasure of hard drives with off-site physical shredding at a secure facility that certifies destruction ensures media is properly destroyed.


Shredding Equipment

Shredding equipment has been used for secure paper document destruction for many years. The shredding of electronic media, particularly hard drives, requires very large specialized equipment, and has only recently become an available service. It is the only absolute method of assuring that the recorded data can never be recovered. Shredding of electronic media is performed as a remote service by professional data destruction companies. The service includes legally important data destruction certification. Hitting a hard drive with a hammer or drilling a hole through it damages the physical hard drive but does not destroy the data recorded on it. Shredding not only destroys the hard drive mechanism but also demolishes the recorded platters.

There are several problems associated with this procedure.

1. Because the equipment is very large, shredding of hard drives and certain types of tape cartridges cannot be performed on-site, which creates a potential security risk associated with shipping.
2. Unlike shredded paper, material from shredded electronic media is difficult to dispose of. In some states the shredded hard drive material may be an environmentally controlled waste.

What's Best For You?

If you are in an industry with clear legal liabilities associated with proper data disposal, documented data destruction is a must. Professional third-party data destruction services that have received appropriate "due diligence" review provide legally strong data destruction documentation. Combining in-house software erasure or degaussing with off-site shredding accomplishes several important security objectives. Initial data destruction efforts are performed under management control and the old media is removed from your premises promptly and on a regular basis. The media is physically destroyed and certified destruction documentation is provided. Such a procedure exemplifies routine good housekeeping that mitigates the legal compliance conundrum. 

Dan Bayha is Vice President of Back Thru the Future Computer Recycling Inc (www.recyclepcs.com), a Department of Environmental Protection-registered electronic recycling firm serving markets nationwide. He is a member of NAID, ISRI and ISSA.

¹ Spoliation is the legal term for evidence destruction