

**Saving money.
And reputation.**

Proper disposal of electronic records



By Daniel F. Bayha

Today, 90 to 95 percent of all business records are stored in electronic format. Because electronic storage is so inexpensive and we use so many different devices, we tend to store everything because it just seems less complicated.

After two to three years of computer or Blackberry use, it is easy to lose track of what information is stored — and where it is located. In the event of litigation, these storage devices are subject to discovery. Professional data discovery technology is fully capable of finding the proverbial “needle in the haystack”. The potential consequences of this type of casual electronic records management are chilling notions at the least.

Filled storage space = mountains of biz records

Electronic data storage technology is racing forward at mind numbing speed. On average, capacity for storage devices will increase at a rate of 50 percent annually. You can now purchase a single hard drive with a capacity of one terabyte (one trillion bytes) for less than \$250. In two years you will be able to buy a hard drive for the same price that will have double the storage capability, holding more than two trillion bytes. Put this tremendous storage potential into perspective: A single gigabyte of electronic storage is equivalent to seventy five thousand typewritten pages. A terabyte hard drive is

comparable to a medium sized warehouse full of paper. Standard mobile phones hold two gigabytes of storage.

Enter the smoking gun

Today, the true 800-pound gorilla posing a very real threat to law firms and their clients is litigation and electronic data discovery (EDD). Courts have been extremely lenient in what they will allow, even permitting forensic data recovery efforts for information deleted from your electronic files. The U.S. District Court of New Jersey Civil Rule 26.1 Discovery subpart d. 3(a) states: “Preservation and production of digital information ... whether restoration of deleted information will be necessary.”

According to Adam Cohen, Senior Management Director in FTI Consulting’s Electronic Evidence Group, “Data destruction saves on cost of discovery. In lots of cases, courts are permitting forensics people to recover data that has been deleted or erased from storage media. Companies have to foot the bill. There is a greater volume of discoverable information. It’s more expensive to do forensics if you don’t destroy the data you’re entitled to destroy.”

By not promptly and absolutely destroying stored information at the end of its retention period, you run the risk of your smoking gun getting caught in an EDD fishing net. Failure to destroy electronically stored information properly, and at the correct

time, will surely lead to higher discovery costs, and can result in a lost lawsuit and even jail. This disturbing matter concerns everyone at a firm using computers or similar devices — mobile phones or personal digital assistant (treasured Blackberry included).

Over 227,000,000 breaches recorded since 2005

A chronology of data breaches found at The Privacy Rights Clearing House (<http://www.privacyrights.org/ar/ChronDataBreaches.htm#CP>) lists reported breaches since 2005. As of this writing, 227,115,680 breaches had been reported. As a result of inadequate attention to electronic records management, we've seen a proliferation of government and industry regulations now requiring the protection of sensitive and personal information — Sarbanes-Oxley, Identity Theft, HIPAA and PCI, for example.

Pound of flesh saved with ounce of prevention

Headlines glaringly expose the risk when sensitive information isn't suitably protected. What firm wants to have a blunder streaked across newspaper front pages? Sound planning will mitigate risk, isn't costly and may be priceless. The first step towards proper electronic records disposal is to adopt a sound document retention/destruction policy and then follow it.

End-of-life records management; apply best practices

The ATA principles of electronic record destruction offer a records management guideline to the proper disposal of electronic documents which will insulate your firm when applied in good faith.

Absolute: When electronic records reach the end of their retention period and approval to destroy has been granted, destroy them *absolutely* in such a manner they can never be recovered by any method — including forensic data recovery.

Proper destruction of electronically stored information is not a trivial technical issue. Different devices require different tools, each of which needs to be applied by a knowledgeable individual. As the storage capacity of devices increase, the time it takes to apply and verify these tools takes longer and longer.

As an example, a high security software data erasure tool will take more than six hours to erase a 100gb hard drive. After all of those resources have been expended, data recovery is still a potential risk.

According to Sonja Robinson, FTI Consulting Director, Forensic Lab Management, "If physical destruction is done properly, it's the best kind of destruction because it's not technology-dependent". Robinson adds, "You can't put it back together again. Platters cut with scissors — that data can be recovered. Software does 'DOD wipes' (7-31 passes) — very good and reliable, but depends on how it's configured and what technology is available. What was good five years ago might not stack up against today's modernized data recovery tools. Data recovery tools can recover one to seven wipes. However, you can't unmelt and unshred a drive." **Timely:** Records destruction should be performed as soon as possible after approval is granted and must be performed on a scheduled basis. Accumulating to-be-destroyed data storage devices is a dangerous practice that can result in having those files caught up in a discovery process.

The scheduling of destruction events is another critical issue. In 2007 Connecticut attorney Philip Russell was charged with misprision of a felony for destroying a client's laptop that contained pornography and which was involved in an investigation. Russell acknowledged he destroyed the computer, but said he did not expect an investigation. If a computer is recycled just prior to knowledge of a litigation event, a question of motivation can arise. We are seeing plaintiff lawyers claiming spoliation of evidence because of ad hoc destruction activity. If your firm has maintained a schedule for destruction/recycling activity, adherence to a schedule is your defense.

Auditable: Detailed, auditable records should support destruction

activity, demonstrating your firm follows a strict and reasonable procedure for the destruction of electronic records.

The federal courts Federal Rules of Civil Procedure Rule 37(d), (3), (e): "Failure to provide electronically stored information — absent exceptional circumstances, the court may not impose sanctions under these rules on a party for failing to provide electronically stored information lost as a result of routine good faith operation of an electronic information system." This is known as the "Safe Harbor data destruction rule." While the federal courts' definition of a safe harbor data destruction event doesn't require auditable records, the ability to support a "routine," "good faith" process will depend on auditable records of your activity.

The authority on records destruction

The current authoritative source for records destruction techniques is the Computer Security Division of the National Institute of Standards and Technology (NIST) publication 800-88 "Guidelines for Media Sanitization," published in 2006. Sanitization is defined as the removal of recorded information from the media it was originally recorded on. In this definitive report, all currently used data storage devices are listed and three levels of sanitization are defined in the order of their effectiveness: Clear (lowest level), Purge (medium level), Physically Destroy (highest level).

Which sanitization level should you choose?

Reuse of old data storage devices should be carefully evaluated. If reuse of a storage device is designated, clearing is generally the only option. Both purging and destruction typically make the device inoperable. Clearing as an option should only be selected if the reuse will occur within your organization. Data recovery forensics can retrieve data from cleared devices and, because of certain limitations of clearing techniques there is a possibility of data not being fully erased from the media. This allows even a non-technical person to see your data. The reuse

of the media outside of your security perimeter steps up the potential that someone somewhere will look at your drive. Reuse internally also enhances the possibility of data forensics recovering old data in a discovery process.

Lessees who return computers at lease end, will often replace their used hard drives with used devices purchased inexpensively over the Internet rather than risk reuse of their drives by the leasing company.

Purging and physical destruction offer medium and high-level sanitization effectiveness respectively, but involve the use of specialized equipment. When performed properly, however, these options offer eminently less risk of exposure. The good news is that these services are easily obtained by outside vendors, at a cost that won't chomp through your budget.

Redundancy of sanitization processes is more effective

All highly secure procedures utilize redundancy of processes to assure 100 percent effectiveness. A current industry best practice for the absolute destruction of recorded data is to clear or purge media onsite. The media is then securely transported to an outside vendor's physical destruction facility for final disposition. An inexpensive yet effective first step is to make the device inoperable by drilling or hitting the device with a hammer and then securely transporting the device for physical destruction.

You shred paper, don't you?

We're familiar with the shredding of paper. Shredding data storage media

and devices is similar but utilizes shredding equipment on steroids. A principal benefit of shredding is that it is a readily available service and it can be an environmentally friendly process if the shredded material is recycled. Other physical destruction methods — pulverization, disintegration and incineration — are typically highly specialized activities and normally are not cost effective for small quantities of media.

Environmental regulations are also a concern. In many states, New Jersey included, the physical destruction of electronic devices is a highly regulated activity and must be performed by a facility licensed by the Department of Environmental Protection. As an example: Unlike paper, shredding of hard drives in a vehicle or onsite at your facility is not permitted in New Jersey.

Timely and scheduled destruction

Escalating costs associated to electronic data discovery strengthens the argument in favor of disciplined data destruction events. Sonja Robinson of FTI states, "Many organizations accumulate old hard drives. These drives are often piled up on an IT person's desk and are low priority items — people don't get around to dealing with them."

Establish a written policy for the destruction of electronic records that keeps to the ATA rules of record disposal as mentioned earlier. Prompt removal of media to be destroyed should be performed on a preset schedule basis. Maintain a schedule, or have a third party service do this for you. Documentation of recurring activity supports your data destruction policy.

Conclusion

The risks associated to improper electronic record disposal have reached unacceptable levels for law professionals and their clients. Taking time to establish (and follow) a records destruction policy providing for the absolute destruction of non-essential electronic records on a timely and scheduled basis and having detailed records supporting your activity will act as strong legal protection from the claims of spoliation of evidence.



Daniel Bayha has spent his entire 35-year business career in the technology field. He joined Back Thru The Future in 1992 as CFO. A frequent speaker on secure data destruction practices, his lecture "Best Practices for Data Security and Sensitive Client Data" was accepted as an accredited course for continuing legal education (CLE) for legal professionals. Reach Back Thru The Future at 973-823-9752; <http://www.safeharborexpress.com>.