

# New Jersey Law Journal

VOL. CLXXXIX—NO.8—INDEX 684

AUGUST 20, 2007

ESTABLISHED 1878

## Law Office Technology

### Shred It or Dread It

Physical data security considerations for New Jersey firms

By Christy Burke

Recently, two New Jersey-based entities suffered major consequences as a result of *physical*, not Internet-based, data exposures. Based upon these examples, New Jersey law firms will certainly have to sit up and take notice.

In May 2007, Alcatel-Lucent was sent reeling from the loss of a CD containing 200,000 names of current and past employees. Lost in shipping between two of Alcatel's vendors, the CD contained not only salary and confidential employee data, but also Social Security numbers. Out of desperation, Alcatel involved both the New Jersey State Police and the U.S. Secret Service to try and track down the missing CD, which is small and portable enough to fit into someone's handbag.

In a different nightmare, the Ewing Township police department had to contain the damage caused by confidential data exposure in which crime-fighting strategies, employee histories, reprimands and other sensitive material were posted to the Internet for all to see. How did this

---

*Burke is with Burke & Company of New York, N.Y., a business consulting firm. The firm represents BTTF, a company discussed in the article.*

information get into the wrong hands? The data was stored on hard drives of the Ewing police department computers that were sold at a town auction for \$16 each. A critic of the local police department purchased a machine and used data recovery software available on the Internet to recover and publish "erased" data.

So how can law firms learn from these examples?

Law firms not only have to practice good data housekeeping from an internal standpoint, but they also must safeguard and protect sensitive client information.

Law firms are document factories — each one churning out contracts, pleadings, briefs and countless other documents every day. This type of data is no longer confined to servers and desktop or laptop computers. It can be found on Blackberrys, on hard drives found in office copiers and printers. Employees wear thumb drives on chains around their neck as if they're office jewelry, oblivious to the risks that come from such a casual attitude toward data protection.

Managing all of these data storage devices is a huge challenge that must be mastered. Failure to do so can result in the public exposure of a law firm or client's data and end up like Alcatel and Ewing — in the middle of a reputation-

damaging scandal.

The New Jersey State Legislature Statute 56:8-162 regarding destruction of certain customer records states that "A business of public entity shall destroy, or arrange for the destruction of, a customer's records within its custody or control containing personal information, which is no longer to be retained by the business or public entity, by shredding, erasing, or otherwise modifying the personal information in those records to make it unreadable, undecipherable or nonreconstructable through generally available means."

Bob Johnson, Executive Director of NAID (National Association for Information Destruction — [www.naidonline.org](http://www.naidonline.org)) says that law firms and businesses "need to pay attention to their *electronic* data disposal just as much as their paper disposal." Johnson says, "Imagine that a company has a tractor-trailer full of documents and dumps them in a landfill without shredding them or taking thorough destruction measures. That's shocking enough, but then imagine that same tractor-trailer full of electronic media (CDs, backup tapes, hard drives, etc.), realizing that each media storage unit holds the equivalent of an entire truckful of paper documents." He comments that the fact that law firms and companies are not focusing enough attention on this as huge potential for exposure is surprising, especially when the news provides overwhelming evidence of its importance.

NAID has certified about 15 ven-

dors in the destruction of electronic data media. One of these certified providers is the Ogdensburg-based Back Thru The Future or "BTTF," ([www.backthruthefuture.com](http://www.backthruthefuture.com)) a state-of-the-art physical data destruction and computer recycling facility located in Sussex County. In addition to being NAID-certified, BTTF has also worked closely with county, state and federal environmental agencies to ensure compliance with waste disposal and "green" issues.

BTTF has developed a secure, auditable data destruction procedure tailored to the needs of law firms and corporate clients. Their trademark procedure is called Safe Harbor Data Destruction<sup>SM</sup> or "SHDD." Through this process, loose and defective hard drives, backup tapes, obsolete PDAs and other data media are collected at the client or law firm's location using secure, locked steel containers. When full, the containers are then shipped to BTTF's facility, at which point they are shred into unrecognizable particles. The final step includes transporting of the shreds to a smelter, where the fragments are melted and recycled into reusable aluminum, and other metals and plastics.

"Destroying data at the end of its lifecycle must be a *process*, not a one-time project; this is important for the destruction activity to qualify as a FRCP (Federal Rules of Civil Procedure) defined 'Safe Harbor' data destruction event," says Dan Bayha, vice president of Back Thru The Future. "It's an ongoing discipline which law firms need to cultivate, and also something they need to advise their clients about."

Bayha points out another issue — the potential cost if obsolete data storage devices are counted as discoverable evidence. Imagine the cost of paying a forensics data recovery firm to go through 365 days' worth of backup tapes, most of which is duplicative information. The cost for such an e-Discovery process could amount to tens of thousands of dollars, or more.

Bayha adds that a majority of the company's law firm clients came to them initially because of loose or defective hard drives that they didn't know how to dispose of. "Loose and defective hard drives are extremely dangerous to keep around because they represent unpurged historic data," says Bayha. "However, most IT people consider them a low-priority item, so the drives stack up on dusty shelves or in storeroom boxes. In the event of litigation, those hard drives can be a gold mine for forensic data recovery specialists."

One of BTTF's customers for the above-mentioned SHDD process is law firm Lester Schwab Katz & Dwyer, LLP or "LSK&D" ([www.lskdnylaw.com](http://www.lskdnylaw.com)), which has offices in Millburn and Manhattan. LSK&D's IT Director is Michael Chung. Chung explains that prior to using the SHDD system, his firm was using a method combining software-based and demagnetization of hard drives to erase the contents. "We used to run a DOS-level formatting of hard drives; then we took a large magnet and ran it over the hard drives to demagnetize them."

Chung says that this "format and demagnetize" system was flawed in several ways. First, it was extremely time-consuming. "Each hard drive would take between 20-60 minutes to reformat for each machine, depending on whether the machine was in working order or not. My staff did each one manually. A mass cleanup of machines could take one of my staff members a whole day for reformatting and testing of all disks."

In addition to the time factor, Chung says that the software-based hard drive erasure method was not completely effective. "Sometimes we would boot up a machine and the hard drive would still be workable. Before we started physically destroying and melting the hard drives, there was no way of guaranteeing that the data was gone from the previous usage. With data media shredding and melting, we

can now be 100% sure that there is no risk of the data being recovered."

Adam Cohen, Senior Managing Director of FTI Consulting's Electronic Evidence Group ([www.fticonsulting.com](http://www.fticonsulting.com)), explains that "Physical data destruction can save on the cost of discovery. In many cases, courts are now permitting forensics people to recover data that has been deleted or erased from storage media, and client 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 when there is no requirement to keep it."

Common sense dictates that used computer equipment and data-containing media shouldn't be simply thrown out with the trash. Reenee Casapulla, Recycling Coordinator of the Sussex Municipal Utilities Authority in Lafayette, calls for the state's law firms and businesses to be more environmentally responsible in their disposal of electronic equipment and data media. She says, "Businesses need to realize their level of responsibility for the level of waste that they generate. Processes such as hard drive shredding, melting and recycling have a favorable impact on the environment if they are properly done. Not only do they prevent materials from being added to landfills, but they also allow for aluminum and other materials to be reused. This reduces the need for new mining of raw materials." Casapulla recommends to law firms and other companies that they seek data disposal vendors that are certified by county, state and federal environmental authorities.

Now more than ever is the time for New Jersey-based law firms and corporations to pay attention to their physical data security and disposal of electronically stored information. By developing a physical data security and disposal plan, law firms can head off disaster and be environmentally responsible at the same time. ■