



NEW TECHNOLOGIES INC.

The Digital Discoverer

Trends in computer forensics & e-discovery for civil litigators

Electronic Document Retention Policies: And Why Your Clients Need Them

BY PAUL FRENCH



In *Residential Funding Corp. v. DeGeorge Fin. Corp.* 306 F.3d 99, the 2d U.S. Circuit Court sounded a grim warning for companies lacking a sound electronic document retention

policy: if you wind up in court and can't produce the goods, you're liable! The 2d Circuit held that where a party breaches a discovery obligation by failing to produce evidence, the trial court has broad discretion in fashioning an appropriate sanction, including the discretion to delay the start of a trial, to declare a mistrial, or to issue an adverse inference instruction. Sanctions may be imposed where a party has not only acted in bad faith or been grossly negligent, *but also through ordinary negligence.* Residential Funding holds that delay, as well as destruction, is sanctionable. Vacating the trial court's sanctions order, the 2d Circuit Court reversed and remanded the plaintiff's favorable \$96.4 million jury verdict because the plaintiff failed to produce certain emails until after the trial had begun...even though the unproduced evidence – email that resided on old backup tapes – was felt to contain little if any significant material for the defense's case.

Ouch!

I get at least 2 or 3 calls a month from law firms or corporate counsel enquiring how

long they should hold on to data – and how they should go about storing and purging data, should the eventuality of a lawsuit arise. There are a several good reasons (beyond dodging sanctions) for advising your clients to establish a digital document retention protocol. An established protocol can lessen your client's liability if implicated in a lawsuit. It can put your client in a position to easily access data that might be exculpatory, or at least, supportive of the company in defense of a claim. Lastly, displaying a pro-active stance toward electronic discovery requests can convey a "we have nothing to hide" spirit that can aid your clients in the court of public opinion.

What to Keep

In the relatively short history of corporate electronic data retention, policies have been fairly straightforward: delete it. This philosophy resulted from the precept that a truly protective policy must mandate the destruction of various types of electronic data upon a fixed timetable. As we've learned from the debacles at Enron, Arthur Andersen and Merrill Lynch (to name a few), this is not a wise protocol. Nor is it wise or cost-effective to retain *all* electronic data. A responsible approach is to shift the focus from "what to destroy" to "what electronic documents to retain". Such a focus makes an excellent foundation for a sound electronic document retention policy.

There are several questions that need to be answered to address the larger question of "what to keep". The first is, "what type of documents and what sort of key words or phrases are deemed sensitive?" The second is, "does the company allow documents to be created and saved on local machines, or is everything saved on a central server(s)?"

Regarding the first question, there are some obvious answers. For example, words

Inside The Digital Discoverer

Inside NTI Pg. 2

Featured Employee: Paul French, Director of Forensic Consulting Services

Making Your Case: Computer Forensics In Action Pg. 4

Public company responds to concerns about financial irregularities

Ask The Experts Pg. 4

What's the difference between a mirror image backup and a copy of data in question?

Video Presentation on Computer Forensics

NOW AVAILABLE



If you've been unable to attend one of NTI's "Webinar" Presentations,

you can now enjoy an 80-minute presentation on the topic of computer forensics and its applications for civil litigation at your own leisure. Account Executive Rich Radford was filmed doing a presentation for the 2003 Asia Pacific Computer Forensics Conference, and now we can make Rich's presentation available to you on CD or DVD. In the coming months, we will also be placing clips of Rich's presentation on www.dataforensics.com for you to download and view. To receive your copy, please call 503-661-6912, or email info@dataforensics.com.

We'd also be happy to schedule an in-house presentation or webinar, if that would better suit your needs.

or phrases that have a sexual or racial content would obviously be deemed sensitive, as they might prove important in an employment law-related case. To isolate e-mails containing such matter, an e-mail filtering program could be customized to search both messages and attachments and save copies of any that contained keywords or phrases deemed sensitive. This would safeguard the organization from relying on end-users to save these messages, and would guarantee that all e-mails are retained in a universal format in a single location. It would also save money and storage space by not archiving *every* message that passes through the company's servers. By indexing these messages and attachments, an organization will greatly streamline future data requests – and save significant dollars in the process.

Your clients might also wish to copy and retain copies of certain file types, depending on the nature of their businesses. For example, a high tech manufacturer who creates potentially patentable designs might want to retain all Acrobat PDF files or other graphics-oriented documents that might contain

design information, should a patent infringement-oriented matter surface.

The question of whether documents are created and saved on local machines or stored exclusively on a central server speaks to the sort of back-up procedures the retention policy should recommend. If files are

“It is a good idea to have an objective third party periodically review and validate that policies are being followed.”

created and saved on local machines, it is possible to set workstations up so that duplicate files are saved on the servers. This gives much better control of potential evidence, as otherwise the organization would need to periodically review the content of each machine, a time-consuming and expen-

sive process.

Another thing to consider in crafting a retention policy is whether or not employees are allowed to take laptops on the road or home, or to work on company business from a home computer. In the case of laptops, synchronization software could be used to update the files on the server the next time the laptop logs into the network, so all information is accounted for. Once the files are on the network, forensic search tools could be deployed to identify key files that would fall under the retention policy. They could then be copied and archived according to the procedures established in the policy. Your clients should consider limiting the accessing of company information at home, as this may necessitate review and archiving of employee's home computers to stay in compliance with retention policies...another headache!

Policing the Policy

A good digital document retention policy is, of course, only as good as the method in which it is implemented. Here are a few po-

Inside NTI:

In each issue, we feature a key NTI employee or an important NTI technology development. This issue we feature:

Paul French
Director of Forensic
Consulting Services



Professional Background: Paul came to NTI in 1999 following a thirteen year career in the U.S. Air Force. He spent his first eight years in the military operating sophisticated computer and communications

systems worldwide. In 1994, Paul transferred to the Office of Special Investigations and became a Special Agent where he performed diverse roles in felony crime investigations, counterintelligence operations, anti-terrorism training and in the computer forensics analysis of government computer systems. Paul is federally certified by the

U.S. Department of Defense to seize, extract, process and document electronic evidence from a variety of Microsoft-based computer operating system platforms. He currently acts as an advisor to the U.S. National Institute of Standards and Technology regarding law enforcement and electronic evidence standards and related issues. Paul has held a Top Secret U.S. Government clearance and holds a Professional Development Certificate from Oregon State University in Computer Forensics.

How He Became Interested In Computer Forensics: I became interested in computer forensics while I was working in the Air Force Office of Special Investigations. If you have a computer background and the inclination, you can become an expert in the analysis of computer media. I've been interested in computers since I was 13, so I jumped at the opportunity. I attribute the broad experience I have gained in dealing with computer evidence from the diversity of the cases I have worked – from complex fraud investigations, to counterintelligence inquiries. My initial training was with Howard Schmidt, one of the pioneers in the field.

Most Memorable Case: It was one of my

first cases at NTI, and involved software piracy through the Russian Mafia. Some Russian mobsters were setting up fictitious publications in the U.S. to get their hands on free, pre-release copies of gaming software – they'd claim they were going to review the games for magazine articles. The “pirates” would take the software, strip out the video and audio code, and then send it back to Europe for duplication. Counsel for the plaintiff – a software rights group – got its hands on the computer of one of the suspected parties and began tinkering with it. I remember telling them, “You know, a lot of these mafia guys booby trap their computers with explosives. Turn it on or open the cover and, BOOM!” The gaping jaw and pasty pale skin of the attorney told me that I had driven home one of our fundamental recommendations – leave computer forensics to the experts. Fortunately, the computer in this investigation wasn't rigged. Once I was able to review the hard drive on the PC, it was fairly easy to locate the strings of communication between the suspect, the software producers, and the pirates abroad.

When he's not investigating: Paul enjoys regional travel and spending time with his family – his wife Kathy, his sons Logan and Ethan, and his Norwegian Elkhound, Bear.

licensing guidelines you should have your clients consider:

- Establish a policing department/task force, so there are easily identifiable “go-to” people regarding retention activities.

- The policing team should create detailed logs of purging and back-up activities.

- Archiving procedures should be periodically reviewed and tested. More times than your clients would care to know, back-ups are not being properly conducted...or aren't being conducted at all. As alluded at the outset of this article, incompetence is not a sound defense strategy! If backup tape hardware is updated, be sure that there's a plan for accessing data on old tapes, as such tapes very likely will not work with the new hardware. Old backup tapes stored in a seldom visited closet could pose an unpleasant surprise if they appear suddenly in discovery proceedings.

- Make certain that all media are considered and accounted for in the purging policy. This includes not only servers, desktops, and laptops, but also PDAs, Blackberrys and various removable media devices.

It's a good idea to have an objective third party periodically

review and validate that policies are being followed. In doing so, the vendor should interview key personnel and review a sampling of data using forensic tools.

If The Call Comes...

Your client might do everything right, operate a distinguished business adhering to all protocols of integrity and fair play...and the lawsuit might still come. In this eventuality, every organization must be prepared to meet the challenges posed by the demand for discovery data – the duty of preservation; the duty of retention and the duty of production. By having an electronic document retention policy in place, and by being able to prove that the policy has been implemented, your client will be prepared. They'll be able to show that general employees of the company as well as the IT Department

are well-schooled in the disciplines of good-faith preservation. There are several other steps your clients can pursue:

- Select and prepare an IT employee of the client to be the designated witness for (in the Federal System) a 30 (b) (6) deposition taken for the purpose of gaining knowledge of a party's computer network and data storage methodology. This individual should be well-schooled in the Retention Protocols and capable of participating in conferences under Rules of Federal Procedure 26 and 16 in order to stipulate to a plan for discovery.

- Secure all storage media containing potentially discoverable data immediately upon demand (including hard drives of PCs and laptops) and take steps to preserve the electronic evidence to avoid claims of spoliation. A generalized preservation plan should be documented. This process should

be carried out in a way that does not place the company's day-to-day business in a state of limbo. Your client might wish to retain forensic experts for the imaging and examination of storage media. The argument here is that, as in paper productions, the opposing side is not entitled to rummage

through a whole real metal file cabinet containing non-relevant documents as well as discoverable ones. The opposing side is likewise not entitled to have its own experts search, at will, through the data on a hard drive in an attempt to extract specific files, whether active or residual.

- Advise your client to keep all personnel with a need to know in the information loop, especially IT people. Make sure they have studied document retention protocols.

There are additional costs associated with the systematic collection and organization of data that a digital document retention policy entails. However, the pro-active outlay of resources can mitigate far greater expenditures down the line.

Just ask the folks at Residential Funding!



NTI Secure
TOOLKIT

NOW AVAILABLE

NTI Secure Toolkit is a Microsoft Windows/95/98/NT/2000/XP-based security program that quickly and easily secures files on notebook and desktop computers through U.S. NIST-tested, 256-bit Automated Encryption Standard (AES) encryption. With NTI Secure Toolkit, users can send secure email file attachments and protect files that are downloadable from Internet FTP sites with assurance that the files will not be accessed without authorization.

Three recently enacted laws by Congress (HIPAA, Graham-Leach-Bliley and Sarbanes-Oxley) require many businesses to establish safeguards and controls over the security and privacy of consumer financial and health information and other sensitive information. NTI Secure Toolkit is an important solution in helping organizations comply with these laws. NTI Secure Toolkit can also secure attorney-client communications stored on computer files.

NTI Secure Toolkit is extremely easy to use. Recipients only need to know a shared password to access encrypted files. They need not have a licensed copy of the software because the software automatically creates a secure, self-extracting decryption program when the correct password is applied.

NTI Secure Toolkit is currently the only encryption software available with a special recovery feature that allows access to encrypted files if the password is lost or forgotten. This special recovery feature is very secure and is only accessible by the organization's security employees.

The encryption technologies employed in NTI Secure Toolkit are so rigorous that NTI is required to restrict the sale of this software to only specific countries; it cannot be sold to the general public. For more information, visit www.secure-data.com/nti-st.html; or call 503-661-6912 and ask for Andrew Batman.

Making Your Case: Computer Forensics In Action

The scenario below is based on an actual NTI case.

Public company responds to concerns about financial irregularities:



An accounting firm was conducting an audit of a publicly-owned company when it came upon some accounting irregularities. The irregularities were serious enough to potentially

necessitate a re-stating of earnings. Considering the many scandals that have blighted the corporate sector, the accounting firm wished to confirm its findings before sounding any public alarms. The firm retained NTI to conduct large-scale data mining to get to the bottom of the irregularities.

Initially, NTI was requested to perform forensics examinations upon scores of the publicly-owned company's computers from locations around the world – a service that would easily add up to over \$100,000 in initial consulting services. Working with the accounting firm and the company, NTI convinced both parties to significantly narrow the universe of computers to be searched; the conjecture was that given the parameters of the matter, any trail of malfeasance would likely lead to the executive ranks. The accounting firm and client agreed. Initial processing revealed sufficient information to enable the public company to meet its fiduciary needs, for a fraction of the initial projected expense.

Ask The Experts

Addressing frequently asked question from clients.

In each issue of The Digital Discoverer, we address a common question our clients have about computer forensics and digital discovery strategies.

Q: “What’s the difference between a mirror image backup and a copy of the data in question? Why should I bother to incur the expense?”

A: Mirror image backups involve the replication of all sectors of a computer hard disk drive, including all files and ambient (or hidden) data storage areas. System or network “copies” focus on files alone. Bit-stream backups are sometimes also referred to as ‘evidence grade’ backups, as the accuracy of the backup must meet evidence standards. To guarantee accuracy, mirror image backup programs rely upon mathematical computations in the validation process. These mathematical validation processes compare the original source data with the restored data.

There are a number of important reasons why we recommend against backups by the IT staff. They are outlined below:

- Specialized forensic imaging software is required to ensure full, validated data captures are accomplished. Virtually all off-the-shelf software that an IT department would own fails to meet these criteria.
- Routine (non-forensic) software used to “copy” data can significantly alter file date information on the source drive. This information is often critical in a computer forensic investigation.
- If improperly used, not only could forensic imaging software miss data, but it could completely overwrite your source (i.e. evidentiary) information.
- People capturing data for use in court

must have evidence handling experience so they can both testify and validate that relevant findings were obtained in a manner consistent with legal standards.

· Many times, it looks bad if the people producing your “best evidence” are also the ones who directly benefit from the content of the information they provide. To eliminate any notion of impropriety, a disinterested third party should be responsible for the collection of the information used to make expert opinions.

· Forensic mirror imaging tools work with data storage hardware at a low level. As such, you often run into technical glitches that only someone experienced in the computer forensic industry could safely and efficiently resolve.

· New tools, techniques, and legal issues/opinions are constantly evolving as it relates to electronic data preservation. It’s our full-time job to keep up with these changes, something no IT department could do given the belt-tightening going on in the IT world.

· Forensic imaging is not just using the software. It involves capturing hardware information, taking detailed investigative notes related to imaging activities, articulating the imaging process in layman’s terms for courtroom presentation, examining hard drive organization and operating system types that will drive the type of processing steps to take, and implementing techniques to image high capacity storage devices (such as RAID’s and large volume hard drives) to minimize setup and processing costs, etc.

· Forensic imaging should be done in a controlled manner, which means using hardware that does not influence the accuracy of your data capture, and through the proper preparation of target media (media/drives that have been forensically “scrubbed” of any residual data).

Go Online!
See What’s On
Our New Website

New Technologies, Inc., a wholly-owned subsidiary of Armor Holdings, Inc. (NYSE:AH), provides digital document discovery services, primarily through computer forensics, to civil litigators. Working with litigation team members as partners we:

- Use forensic processes to cost-effectively manage electronic discovery efforts.
- Consult with you to determine what electronic information is valuable to a case, and how to get it in admissible format.
- Use various forensics procedures (with software tools we’ve developed) to find evidence on computer hard drives and other storage media.

Contact Us At:

Tel: 503-661-6912

E-mail: info@dataforensics.com

Web: www.dataforensics.com



NEW TECHNOLOGIES INC.