

CALSM NEWS

www.calsm.org

Chain of Custody: A Sound Defense Measure

by Bruce Malter

A common summer camp game for children to play is a story telling game where the children sit in a big circle and one child makes up a story and tells it to the child sitting beside them - the game of "Telephone." The story continues to be told to each subsequent child until it circles back to the first child. The fun of Telephone is to find out how the story has changed during its course of travel.

In much the same way electronic data can change considerably from its initial acquisition through delivery to opposing counsel.

As the data changes, the attorneys have more reason to argue the validity and quality of documents being produced. A common argument today, by the party seeking the documents, is "spoliation." Spoliation is defined by Findlaw.com as:

- (1) the destruction, alteration, or mutilation of evidence especially by a party for whom the evidence is damaging, and
- (2) alteration or mutilation of an instrument, such as a will for example, by one who is not a party to the instrument.

During the course of litigation there will likely be protective orders entered and arguments made as to the burdens and expenses of both parties and to spoliation of the documents or data. The seeking party can also expect the producing party to argue that the seeking party's discovery request is overbroad and unduly burdensome.

Federal Rules of Civil Procedure 26(a) and 34 (and similar State rules) are the legal evidentiary rules most closely associated with discovery. The rules require the parties in litigation to confer with each other to develop a proposed discovery plan. Rule 26(a)(1) requires disclosure of documents, data compilations and other tangible things that the parties may use to support their claims, defenses or damages computations. Rule

34(a) allows the seeking party to ask the producing party to produce "data compilations from which information can be obtained, translated, if necessary, by the respondent through detection devices into reasonably usable form."

In other words, a company's e-mail records and its electronic data systems are fair game for discovery. In addition, the seeking party is also entitled to know how the information was collected. Therefore, a sound, well documented and defensible chain of custody is critical to the validity of the electronic data being produced.

The following is a definition of "chain of custody" from Wikipedia, the free encyclopedia:

Chain of custody is a concept in jurisprudence which applies to the handling of evidence and its integrity. Chain of custody also refers to the document or paper trail, showing the seizure, custody, control, transfer, analysis, and disposition of physical and electronic evidence. Because evidence can be used in court to convict persons of crimes, it must be handled in a scrupulously careful manner to avoid later allegations of tampering or misconduct which can compromise the case of the prosecution toward acquittal or to overturning a guilty verdict upon appeal. An identifiable person must always have the physical custody of a piece of evidence. In practice, this means that a police officer or detective will take charge of a piece of evidence, document its collection, and hand it over to an evidence clerk for storage in a secure place. These transactions, and every succeeding transaction between the collection of the evidence and its appearance in court, should be completely documented chronologically in order to withstand legal challenges to the authenticity of the evidence.

Documentation should include the conditions under which the evidence is gathered, the identity of evidence

CHICAGO ASSOCIATION OF
LITIGATION
SUPPORT MANAGERS

Fall–Winter Newsletter 2004

Officers:

President–Barbara C. Hanahan,
bhanahan@winston.com

Vice President for Newsletter–

James B. Salla,
jsalla@jenner.com

Vice President for Membership–

Joanne Kloepfel,
jkloepfel@clausen.com

Co-Vice President for

Programming–
Sarah Mallon,
smallon@sachnoff.com

Co-Vice President for Programming–

Michael G. Weiler,
mweiler@mhmlaw.com

Secretary–Rosede A. Olson,

ROlson@Sachnoff.com

Treasurer–Joni K. Eskridge,

jeskridg@skadden.com

In This Issue: Chain of Command: A Sound Defense Measure

Bruce Malterpg 1

What's Your Measurements?

by Bob Sweatpg 3

handlers, duration of evidence custody, security conditions while handling or storing the evidence, and how evidence is transferred to subsequent custodians of the evidence for each link in the chain.

The producing party and the seeking party each must be prepared to disclose their chain of custody plans. If one of the parties has a more thoughtful, structured and sound plan, that party may be seen by the court in a better light. Therefore, the producing party should take a pro-active approach to the chain of custody. Courts may not favor those without a sound plan.

Producing parties often incorrectly perceive the collection and review of electronic documents as expensive and time consuming. In addition, producing parties are afraid of over-producing sensitive documents that can be perceived as the smoking gun. Chain of custody, however, is not in place to find specific documents, but rather to maintain and document the flow of the electronic data and hardware.

As every case is different and the collection of electronic documents may be handled in different ways, the electronic documents may reach the party's hands with many open questions. The volume of data is not going to be known outright, as an example. Nevertheless, whether the matter is a large or small case, it is equally important to plan and document from the outset.

For a small case, the argument can center on the details of the limited scope. A small case tends to involve only a few computers or back up tapes. These cases tend to go deeper into the data files of the computer. The seeking party also has more specific details on each piece of hardware.

A large case can become quite burdensome as a result of the time frame of the case and the quantity of information. In such a case, the collection and tracking of hardware and data can take months, if not years to complete. In addition, the volume of data is often enormous. Once the data is collected electronically, it can be converted into a reviewable format, most likely with the assistance of an outside vendor specializing in conversion. The more planning and structure around the data collection and conversion, the more the processing stage will be efficient and the costs more reasonable.

Chain of custody is a plan that begins the day notice is received or issued.

A well documented plan to detail every step along the way is one of the key components to a successful discovery and review process, be it for either party in litigation, the plaintiff or the defendant. One should imagine handling electronic data in a similar manner that criminal evidence is handled in a crime case; i.e. very carefully. "Fingerprints" on the evidence should similarly be avoided at all costs.

HOW TO PLAN YOUR CHAIN OF CUSTODY

A plan for Chain of Custody has should be initiated before any data is collected. Acquire a chain of custody document (a qualified forensic expert can help you) or create a document that includes all the necessary information to track all hardware (see below). Establish a procedure to ensure that each party is accountable for logging in and logging out the hardware. Designate and train a 30(b)(6) witness to answer technical questions:

- Advise witness of legal importance of data storage/backup

procedures and data retention/destruction protocols.

- Inventory IT systems, including operating systems, all software and hardware in use, backup schedules, segregation of data, etc.
- Develop clear outline of IT roles and responsibilities as they may relate to legal issues and electronic document production obligations.
- Explain significance of coordination between technical needs and legal needs.

Rule 702 of the Federal Rules of Evidence state that in order for a witness to be qualified as an expert, the expert must be shown to have knowledge, skill, experience, training or education regarding the subject matter involved

Before Collecting

1. Identify all data points including computers, servers, back up media and other discoverable devices
2. Determine where data resides and how it will be collected
3. Inventory every computer, server, backup device and other discoverable media. This document should accompany the associated media along the way. The following information should always be included:
 - Current computer user (and associated contact information)
 - Dates used
 - Previous user
 - Dates used
 - Computer: Type/Model/Serial Number (if the hard drive is accessible also collect the hard drive serial number)
 - Date computer was put into service
 - Date computer was put out of service
 - Operating System
 - Software applications (most common)
 - Date of initial inventory
 - Date of collection
 - Collection method
 - Media copied to
 - Also each person involved should sign and date the document

When Collecting

1. Use the original inventory list to verify every hardware component
2. Confirm all information
3. Document current dates and times
4. If collecting from opposing party, have the supervisor sign and date

Case law mandates that computer evidence be collected in a forensically sound manner and that the proper preservation and chain of custody of computer evidence be established. The court also stated that parties have "a duty to utilize the method which would yield the most complete and accurate results, see *Gates Rubber Co. v. Bando Chemical Indus., Ltd.*"

Benefits of chain of custody

1. Detailed history: cases can go on for a long time,
2. A large collection may have multiple people performing the collection,
3. Allows for metrics - this helps with budgeting and choosing the proper vendors,
4. It provides the vendors the details they need to provide an accurate quote, and be able to manage the data in an efficient manner,
5. Keeps the information catalogued,
6. Ensures evidence admissibility,
7. Allows the Producing party to have a sound defense.

Federal Rule of Evidence 901(a) states: "The requirement of authentication or identification as a condition precedent to admissibility is satisfied by evidence sufficient to support a finding that the matter in question is what its proponent claims." One way to establish that fact is to show the 'chain of custody.' *United States v. Grant*," 967 F.2d 81, 83 (2nd Cir. 1992)

When it comes to computer data, a meticulously documented chain of custody can convince a court that evidence is authentic. After all, "[t]he purpose of the chain of custody rule is to insure that the substance offered into evidence is in substantially the same condition as when it was seized." *United States v. Santiago*," 534 F.2d 768, 769 (7th Cir. 1976) (citing "*United States v. Brown*," 482 F.2d 1226 (8th Cir. 1973)).

CONCLUSION

The best offense is a good defense. A solid, well-documented Chain of Custody plan will minimize the arguments within discovery. Many courts automatically assume that an undue burden or expense may arise simply because electronic evidence is involved.

Chain of Custody allows the producing party to maintain costs, manage budgets and manage the flow of information. Remember that Chain of Custody does nothing to help to find the smoking gun, however the producing party will always have the opportunity to review all data and documents before producing to opposing counsel. Managing the electronic data and using a well documented chain of custody plan is a strategy to give counsel a sound defense.

Bruce Malter is an Electronic Data Discovery and Forensic expert with Project Leadership Associates, Inc. (www.projectleadership.net), based in Chicago

WHAT'S YOUR MEASUREMENTS?

Version 2.0

by Bob Sweat (c) 2004

This article was first published in the newsletter of the Dallas Area Paralegal Association.

I call this Version 2.0 like the software companies do when they release updated versions of their products, as I originally wrote a similar article in 2002. At that time, not much was known about the relation of electronic documents to page counts. Since then, the processing of millions of pages of E-discovery (electronic documents) has provided sufficient data to make reliable estimates based upon those experiences. Of course, we're talking about how to determine the number of pages for an electronic collection. But first, let's review and update paper collection estimates.

PAPER COLLECTIONS THE GUESSTIMATING METHOD

The following is typical for guesstimating paper collections where the box or drawer is full:

• Legal/Letter Box	2,500 pages
• Long Bankers/Transfer File Box	4,500 pages
• Vertical File Drawer 18"	3,600 pages
• Vertical File Drawer 24"	4,500 pages
• Lateral File Drawer 36"	6,000 pages
• Lateral File Drawer 48"	8,000 pages

How many times has your attorney asked, "How many pages do we have?" How many times have you asked a vendor, "What will it cost and how long will it take?" How many times have you heard "IT DEPENDS?" It depends largely upon the total estimated number of pages and the deadline when you need it completed. The rest is a matter of throughput calculations based on the number of machines and personnel available to accomplish the task.

Below is another method you can use to estimate the size of your paper collections. It is based on pages per linear inch. Take your measurements by putting your hand behind the files and gently pressing them forward, then measure the number of inches of paper and use the multiplier below.

THE PAPER MEASUREMENT MULTIPLIER

Type of Paper	Pages per Inch
Photocopies, no bindings	248
Photocopies, with binding elements	225
Originals, w/bindings and folders	200

A ream of standard 20-lb paper contains 500 sheets and measures 2 inches for 250 pages per inch. Of course, the paper is tightly compressed and contains no printing, binding elements or folders. Printing adds very little expansion, while binding elements and folders do add thickness resulting in the lower multiplier used.

In my 2002 article I wrote that there is no way to even guess at how many pages are involved with e-discovery electronic files! Much has been learned from experience in handling millions of pages since that time, providing some indications that may be used to estimate electronic document collections.

“E-DISCOVERY” – ELECTRONIC DOCUMENTS HOW DO YOU ESTIMATE IT?

1 Megabyte (MB)	will average around	75 pages
1 Gigabyte (GB)	will average around	75,000 pages
1 Terabyte (TB)	will average around	75,000,000 pages

Email	average 1-2 pages	per each
Word Processing File	average 5-8 pages	per each
Spreadsheets	average 15-30 pages	per each
Presentation	average 12-24 pages	per each
Graphic	average 1	page per each
Adobe PDF File	average 35	pages per each

Diskette	1.44 MB	if full	50-150 pgs
Zip Disk	100 MB or 250 MB	if full	7,500-18,750 pgs
CD	640 MB - 800 MB	if full	48,000-64,000 pgs
DVD	4.7 GB - 17 GB	if full	350,000 - 1.3 million
Tape Drive	2 GB - 360 GB	if full	150,000 - 27 million
Hard Drive	20 GB and over	if full	1.5 million and up

Now, please, this is not an exact science and someone will surely measure or determine his or her collection to find a different number. Remember, we're talking estimates here.

Electronic files are received without regard to order or type. The vendor should review the directory listings to determine the number and sizes of the various file-types. Once a file list analysis is performed the attorney can utilize the information to determine which files to review before converting to image or paper, providing greater control over the cost involved in processing e-discovery. Applications or system files may be of little value and not worth processing.

Good estimates help to avoid problems when the vendor provides discounts for size and collection is substantially smaller or when the collection is substantially larger than estimated and your attorney must go back to the client for additional funding as a result.

Bob Sweat received his education in Business Administration and Economics at the University of Wisconsin and advanced work at Purdue University. He holds a Paralegal Certificate in Civil Litigation with Computer Emphasis from The Center for Legal Technology, MBTI, Milwaukee, WI, and has 16 years experience working with local and national vendors on large, complex litigations. Bob is currently a partner and Automated Litigation Specialist at Open Door Solutions, LLP, Dallas, Texas.