

**CyberControls, LLC™**

**Providers of digital data discovery services**



## E-Discovery in Civil Litigation

In a recent interview with attorney/e-discovery guru George Socha, he shared the following: "It has been estimated that although more than 265,000 civil cases were filed in Federal courts in 2002, significant levels of electronic discovery are likely to take place in only about 5,000 of those cases. If those figures are correct, at the Federal level electronic discovery is taking place in less than 2% of the cases filed."<sup>1</sup>

Judge Sidney Schenkier of the U.S. District Court for Northern Illinois spoke at an e-discovery conference in late April of 2004<sup>2</sup>, and offered his personal theory as to why most lawyers still hesitate to include e-discovery in civil litigation matters:

1. Lawyers simply do not possess enough knowledge about electronic evidence discovery and how to implement it into their case strategies.
2. Lawyers are fearful to launch an e-discovery request because they anticipate a boomerang request to be launched right back at their own client.

<sup>1</sup> Discovery Resources.org May, 2004

<sup>2</sup> Law Bulletin, "e-Discovery Conference" – Chicago, IL/ April 27, 2004

## The Beaten Path

In today's digital world, studies on the actual volume of all documents and e-mails generated throughout the world and stored on computers is over 93%. Of that volume of data, it is estimated that less than .003% is ever printed on paper.

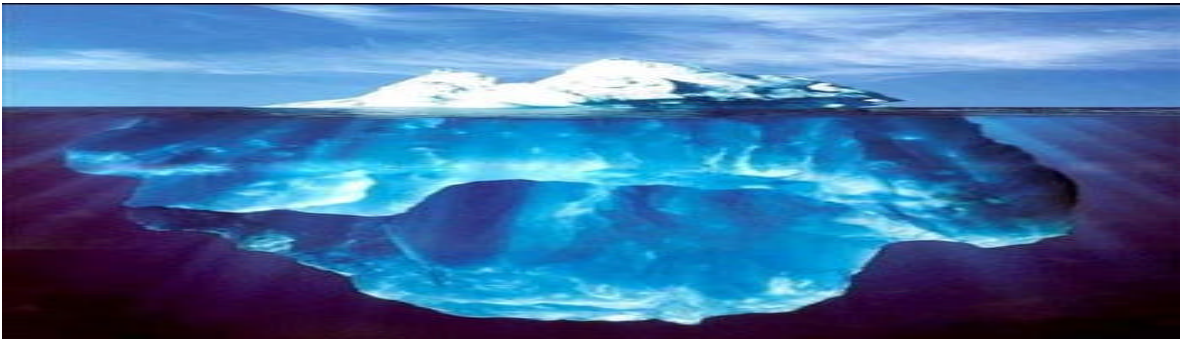
Requesting party's in the e-discovery stage of a case have three categories of evidence in which to pursue:

1. Paper Documents
2. Active electronic documents/e-mails
3. Deleted e-documents/e-mails

The producing party having to respond to an e-discovery request is required to:

1. Preserve all potential evidence
2. Locate all requested data/e-mail
3. Collect all requested data/e-mail
4. Conduct a privilege review of all data
5. Create and submit a privilege log
6. Produce documents/e-mails

*"The definition of insanity is doing things the same way and expecting different results."*



## A Sea of Icebergs

CyberControls' iceberg logo has served to be a universal symbol of the complex world of digital data discovery. With the exponential growth of data and e-mail in the business world, requesting and reviewing "active" only documents and e-mails can often equate to being the "tip of the iceberg." Just how many icebergs have you passed by without ever looking below the surface?

## Deleted Files are Fair Game

For those of us in the digital evidence discovery industry, not a week goes by where there isn't a news article or TV story about computer forensics in a high-profile criminal or civil court case. Yet, many attorneys, business owners, and executives don't have much familiarity with the fact that deleted documents and e-mails are potentially recoverable. The significance of this reality should no longer be overlooked in disputes where electronic documents are already being requested and produced.

CyberControls' team of computer forensic specialists is trained in providing rapid acquisition of digital evidence across the United States. Once the evidence drives have been acquired, the forensic examination team members conduct their

search and analysis for relevant data and e-mails.

## Producing Party Considerations

Evidence preservation is one of the first priorities that should be addressed. For the attorney in this situation, tremendous responsibility and potential liability start with the attorney's detailed instructions covering all possible scenarios covered by an evidence preservation request or order. Ultimately, the responsibility of evidence preservation will depend on whether or not the litigant takes proper precautions to avoid inadvertent spoliation of any relevant evidence. This creates the potential for risk.

Our recommendation to the producing party is to retain CyberControls immediately upon an evidence preservation condition to perform a forensic bitstream copy of all targeted hard drives in which the e-documents and e-mails reside. This cost effective approach will ensure effective preservation of all potential evidence while providing the attorney with an opportunity to also review deleted data for privilege that might otherwise be overlooked.

CyberControls has had occasions in which deleted exculpatory evidence was recovered resulting in a favorable judgment for the producing party.



## Requesting Party Considerations

Nothing less than a full outright plan of attack will prepare you for success. As part of that preparation, CyberControls is poised to assist your e-discovery request to include the deleted documents and e-mails necessary to support your client's case.

## Pre-Filing Support

From the start, CyberControls is equipped to lend support in formulating a strategy that will include plans to conduct a computer forensic examination of the opponent's data. Such preparations might include assistance in the drafting of:

1. Notice to Preserve Evidence
2. Research of the opponent's IT
3. Pleadings and motions with specificity to e-evidence
4. Drafting interrogatories for technology oriented witnesses
5. Protective orders & Ex Parte orders with specificity to e-evidence

## Evidence Acquisition

Once the green light has been given to go and acquire the opponent's data, all eyes are on the computer forensics team. At CyberControls, all necessary preparations are meticulously attended to. Seasoned

professionals are dispatched with every available forensic device required to accomplish a successful acquisition of all targeted media storage devices in a single trip. Strict adherence to forensically sound procedures is followed to assure complete admissibility of any evidence acquired. Chain of custody protocol is never compromised throughout the entire engagement.

## Evidence Examination and Analysis

As part of CyberControls' examination procedures, all acquired evidence transferred to the Forensics Lab is duplicated a second time for precautionary measures before the examination work commences.

An initial inventory is conducted to identify all software applications and hardware components having an existing or past interaction with the evidence media. In addition, a thorough search for any virus, Trojan horse, worms, spyware, or hard drive scrubbing utilities is conducted and documented for future considerations.

The searching process follows after a comprehensive list of search terms have been compiled through a close collaboration between the litigation team, the litigant, and the forensic examiner. The search stage can take a few hours or several days.



## Forward Momentum

The wheels of justice can at times, turn at an agonizingly slow pace. At CyberControls, the throttle is set to deliver results quickly without jeopardizing a favorable outcome. This is accomplished through effective communications and attention to details. The attorney is always assured of maintaining control throughout the process and the engagement's estimated budget is never exceeded without prior approval.

The sooner that CyberControls is able to deliver the results of its forensics analysis to the litigation team the more likely a settlement to the dispute can be reached. Our project managers and examiners are accustomed to working under contracted timelines where an impartial discovery conclusion is required. This is the nature of litigation support and CyberControls is ready to serve you.

## Expert Witness Support

Throughout the entire digital evidence acquisition and examination process, all steps and procedures are precisely documented. Chain of custody logs are maintained to ensure that all evidence is secured and accounted for. Analysis findings are generated and reviewed for accuracy.

Should an engagement with CyberControls require the services of an Expert Witness, he/she will be prepared to present their findings based upon the reliance of strict accordance to the court approved forensic practices followed at CyberControls.

CyberControls' Expert Witness availability is provided to present and validate admissible evidence as well as to refute and challenge the findings of other experts who have not followed sound forensic procedures.

## Qualifying Digital Evidence Discovery

Not every civil dispute will require the inclusion of computer forensics for evidence discovery. On the other hand, most cases require the request for specific data that may or may not be readily accessible to the producing party to be in full compliance with such a request. Using CyberControls even on a limited basis can be the best solution.

For cases that require extensive data discovery, CyberControls is equipped to conduct preliminary examinations of relevant data over a company's computer network. This approach helps examiners to identify specific computers in the network that should be forensically acquired.



## Data Evidence Considerations

The options available to business and individuals when it comes to storing data for future retrieval are constantly growing, so too, is the volume of data being stored. In fact, experts estimate that the volume of data being produced and stored equates to over 250 MB. for every man, woman, and child in the world.

Computer hard disk drives are the most common data storage device in use today. Technology and manufacturing advancements have resulted in storage space recently dropping below \$1 per Gigabyte. In addition, the emergence of portable data storage devices such as external hard drives, thumb drives, CDs, DVDs, PDAs (Palm & HP), and Smart Phones are becoming targeted for evidentiary examination. CyberControls' lab facility and examiners are equipped to conduct data recovery from these devices as well as hard drives and back-up tapes.

## Logical Fit for Computer Forensics

First, computer forensics is an ideal solution for all producing party's who want to avoid any possibility of inadvertent e-evidence spoliation in a civil litigation matter. By securing a forensic copy of all targeted hard

drives and other storage devices, the client is protected. Once this is accomplished, the attorney has the option to conduct a review of any deleted documents and e-mails in addition to active files.

For e-discovery requesting parties, virtually all areas of specialized law practice will benefit from intensive analysis of recovered evidence pertaining to their case such as:

1. Civil & Complex Commercial Litigation
2. Employment Litigation
3. Insurance Litigation
4. Bankruptcy & Financial Law
5. Family Law
6. Product Liability Litigation
7. Real Estate Litigation
8. Corporate Criminal Investigations
9. Technology Law & Litigation
10. Healthcare Litigation
11. Malpractice Litigation
12. Mergers & Acquisitions
13. Banking Litigation
14. IP/Trade Secret Litigation
15. Antitrust & Competition Litigation

## CyberControls' Contact Info:

CyberControls, LLC™  
18-3 East Dundee Rd., Suite 302  
Barrington, IL 60010-5278  
847-756-4890-Office/Lab  
847-620-2500-FAX  
[www.cybercontrols.com](http://www.cybercontrols.com)