

E-Discovery's Primary Hindrance



Boomerang - a miscalculation that recoils on its maker

In practicing law, a miscalculation can often result in adverse consequences. Such is the case when it comes to launching a comprehensive electronic discovery request upon an opponent. Most experienced litigators have learned that basic defense 101 is that *the best defense is a good offense*. In fact, it is for this very reason that most plaintiff attorneys are reluctant to advance an aggressive e-discovery attack upon the producing party-for fear that the defense will retaliate with an equally in-depth e-discovery request. Hence, the potential carnage of the boomerang effect squelches even the most ardent advocate of electronic evidence discovery. In the absence of an in-depth electronic evidence discovery being launched by the plaintiff, it is implicit that opposing counsel will respond in kind - a quid pro quo.

This arrangement has existed for a long time with mixed results. Surely, there have been numerous calamities that were all together avoided by simply not pursuing intensive electronic discovery in civil cases in the past. In today's digital information age however, one has to wonder how many cases would have had a different outcome had there been more pressure exerted on the pursuit of data evidence. After all, it is well known that over 93% of all business data is stored on computer hard drives.

In order to break free of this quagmire, a new dynamic must be added to the mix. For the plaintiff side, there is significant advantage in being the party who controls the timing of when the lawsuit is filed. With exception to certain circumstances that require an immediate filing for relief, the delay of a week to ten days may be sufficient to tackle a critical, first-stage task.

Do you remember being told the old lesson: *those who live in glass houses shouldn't throw stones*. When it comes to launching an all out electronic/data forensic discovery upon an opponent, you will likely upset some folks on the other side. The producing party will have to identify, locate, duplicate, and review each and every document and e-mail before producing them. It will require considerable time, resources and money to complete such an undertaking. Can you imagine what it would be like if your client had to all of a sudden be put through the same fire drill?

So, it would make sense that before the lawsuit was even filed, a thorough review of the various scenarios that might result from an e-discovery strategy with the client. Some important topics worthy of discussion might be:

- The high probability of a retaliatory e-discovery attack
- The need to anticipate and list all e-info that the opponent would likely request
- The importance of formulating a response plan to deal with an e-discovery request
- The need to retain the services of a data forensics service provider to assist in the early planning stages to understand the role of digital evidence discovery in their case

Once the client has sufficient familiarity with what's at stake in approving an e-discovery attack, the next step before filing the lawsuit is make sure that client takes the necessary steps to get their house in order to sustain an e-discovery attack. The importance of attorney supervision throughout this preparation stage is critical to the success of subsequent events. The careful attention to the following action points will help avoid costly setbacks:

- Suggest to the client that they assign key individuals with specific responsibilities as part of a response team to an e-discovery production request
- Insist upon the response team members having to sign an NDA or Confidentiality agreement to keep the future filing secret
- Review with the client whether their business has any formal policies that cover document retention and destruction procedures -and whether these procedures have been stringently followed
- Once the gathering of all data (documents, e-mails, memos, spreadsheets, etc.) that the client has inventoried as being potentially of interest to the adversarial party, it should be copied and moved to an isolated computer or server for future review and retrieval for possible production

“The one who first occupies the battlefield awaiting the enemy is at ease. The one who comes later and rushes into battle is fatigued.”

-Sun Tzu-Year 4 A.D.

Running almost parallel to these precautionary measures, the litigator has a few other options to consider again, before the lawsuit has been filed:

- Conducting an investigation of the opponent’s information technology and business practices and procedures relating to the employee use of computers, networks, and e-mails to help develop interrogatory drafts for future depositions
- Conducting a computer forensic examination of any ex-employee’s company computers relating to the upcoming lawsuit
- Drafting a comprehensive notice to preserve evidence citing all possible data storage devices and routine operational procedures that might result in inadvertent spoliation
- Drafting a protective order that would incorporate the forensic imaging of all data storage devices in custody of the opponent that is in serious jeopardy of spoliation
- Research and review all prior civil cases involving the opponent in which, e-discovery requests and deposed witnesses who provided testimony about their company’s information technology systems and/or procedures for comparative analysis
- Attempt to identify all witnesses for deposition that will provide precise details on the IT facts required to conduct the upcoming e-discovery strategy

Even if your opponent has psychic powers when it comes to anticipating an impending lawsuit, they will never be able to foresee the extensiveness of your thorough preparations.

So why is all of this pre-filing preparation necessary-especially when the case is relatively small or you’re not quite certain what e-evidence or how much of it is likely to exist?

Because, no case is too small if critical evidence resides on a computer hard drive or backup tape belonging to your opponent. As for the volume of recoverable, relevant evidence that may exist is anyone’s guess. There are numerous examples of cases that CyberControls has been involved in where no sooner did our forensic examiner

complete the imagings of evidence hard drives did the opposing counsel choose to enter into settlement negotiations thus halting any examination of their data. You just don’t know what you’ll find until you put the wheels in motion.

Visit our website at www.cybercontrols.net to continue learning about the next steps in activating the e-discovery attack, dealing with complex IT infrastructures, effective pleadings, and conducting computer forensics on a shoestring budget.

Or, you can contact one of our data forensic consultants at 847-756-4890.

Article written by: Robert B. Guinaugh, Managing Partner at CyberControls, LLC™