

CyberBytes



SUBJECT: ADMISSIBLE EVIDENCE

Now that most litigators are sufficiently aware of the fact that requesting documents and e-mails in an electronic format in discovery has numerous advantages over paper-only, it's time to consider adding one more dimension to the request— ALL DELETED DATA FILES — relevant to the case. Consider the fact that opposing counsel is unlikely to have any knowledge of what data files may have been deleted on his/her client's computers—so why would you accept anything less than a thorough examination of the contents of every hard drive for both active and deleted data files pertaining to the case?

By notifying opposing counsel of the extensiveness of your intended discovery examination for relevant evidence, the producing party must take all necessary precautions to avoid inadvertent spoliation of electronic data on those computers and servers on which the active and deleted data of interest exists.

Knowing what specific data and on which computers relevant electronic evidence is likely to be stored can only come to light if you are thinking about discovery on those terms. Considering the fact that over 93% of all business related documents and e-mails are created on computers, it makes sense that a careful examination of deleted files and e-mails for relevant evidence should be an imperative.

Costs associated with computer forensic discovery efforts are often anticipated by lawyers to be cost

prohibitive for the majority of cases. The cost of data forensics is directly linked to how well the attorney is prepared to pursue electronic discovery. For early stage preparation, CyberControls offers its "**E-Discovery Checklist**" for your review. Remember, if the importance of recovering specific documents or e-mails is critical to prevailing in your case, then it will be rather simplistic to arrive at an acceptable budget for data forensic services.

In the absence of requesting an examination of all relevant active and **deleted** data files in your discovery requests, the producing party is obliged to only make a best effort to identify and produce active files off of computers and back-up tapes where they believe the responsive data is stored. Potentially, that leaves a lot of other relevant evidence untouched.

If your client has to win the case and you are considering whether or not there may be deleted data on someone's computer that would be useful to you, you have nothing to lose in exploring how digital forensics might play a role.

Don't wait any longer in exploring the possibilities as to how computer forensic discovery can support your most difficult cases. Call and ask to speak with one of our forensic consultants for an assessment as to how computer forensics may be a fit for a particular legal matter at **847-756-4890**, or see us on the web at www.cybercontrols.net.