Disproving 7 Myths Related to Electronic Discovery

Myth 1 – Electronic Discovery is so difficult it is not worth the time

In reality, electronic discovery is a simple process that is easier and often less expensive to work with than paper. Once relevant electronic information has been identified, legal professionals can review it from their computers rather than sifting through thousands of pages of paper.

Myth 2 – Electronic discovery is extremely expensive

Although the process of identifying relevant documents can be expensive, once they are found it is much less expensive to keep the documents in their electronic form. When these documents remain in electronic form, significantly high costs are removed as printing, shipping, copying, storing, Bates stamping, coding, and scanning costs are eliminated, resulting in an average savings of 85%.

Myth 3 – Electronic discovery is not relevant for smaller cases

Most computer forensic companies utilize volume-based pricing thus, the smaller the case, the lower the costs. Therefore, even smaller cases can be assisted from the benefits of electronic discovery.

Myth 4 – Meta data can be harmful

Metadata is basically data about data. Specifically, metadata describes how, when, and by whom a particular electronic file was created, modified, and where it was transmitted.
These technical aspects of a file often yield information and insight relevant to an investigation or litigation as it conveys a detailed account of a document's history and distribution.
Additionally, metadata can often reconstruct a timeline of events, produce additional investigative leads, and establish a user's knowledge regarding the existence and content of files.

Myth 5 – Conventional discovery provides everything we need to win a case

Although this may have been true in the past, electronic evidence is now often key to winning cases, as it generally includes information that has been deleted after a backup has been made.
In addition, because many organizations are utilizing paperless business systems, much data no longer occurs in paper form. Therefore, attempting to obtain data through paper discovery will not yield as much information as it would through electronic discovery, as many documents will never have been printed. Certain types of misconduct, such as theft of trade secrets, are often only accomplished via computer systems as well, thus the only way of substantiating such an occurrence is through a forensic investigation and analysis of electronic evidence.

Corporate Headquarters
8391 Beverly Blvd. #167, Los Angeles, CA 90048
Tel 323.939.5598 Toll-Free 800.748.5440 Fax 323.939.5481
www.SetecInvestigations.com

Myth 6 – The opposing party won't provide us with electronic information

Once a motion for electronic discovery has been granted, the typical rules of discovery hold true. Electronic information should be easier to obtain, since it is formally catalogued and is usually available to numerous people within the organization, little burden can be claimed as electronic information can be transferred in a matter of minutes rather than copying thousands of pages of paper, and it can be easily searched for using keywords and phrases to ensure its relevance.

Myth 7 – Everything I need will be provided by my client's IT department

The IT staff must be specifically informed as to the proper steps and processes to be followed in order to preserve and safeguard electronic evidence. If the IT staff does not know about the investigation, evidence may be destroyed through daily business operations, such as turning on the computer in question, which may alter information. In addition, it is unlikely that the IT staff will have the necessary training and tools needed to obtain evidence from specific areas, such as log files, registries, temporary files and unallocated storage, or to testify in the event that the case goes to trial; therefore, outside forensic experts may need to be retained.