Learning from Other's Mistakes: Issues Arising from Electronic Discovery

Computer forensics and the associated electronic evidence and electronic discovery are relatively new to the litigation game. The use of such information is growing steadily and it has become impossible for legal professionals or their clients to claim that they are unaware of the existence of electronic information. The following intends to make clear mistakes involving computer forensics, electronic evidence, and electronic discovery that are often made:

Issue 1: Ignoring electronic information or attempting discovery of it in a disorganized manner

As almost all written information is now stored in electronic form rather than hard copy form, it is important for legal professionals to understand what electronic evidence is, how it can be identified, how it can be utilized to enhance a case, how to avoid the pitfalls associated with it, and how to avoid sanctions resulting from inadequately presenting it. When properly planned for, gathered, analyzed, and produced, almost every case would benefit from the utilization of electronic evidence.

Issue 2: Believing that deleted information is actually irreparably destroyed

Electronic evidence that has been "deleted" is rarely actually destroyed, as every electronic document leaves a fingerprint that is stored in unallocated space, as well as other locations on the computer hard drive. Even after information is "deleted" this fingerprint remains, and some semblance of it can usually be identified even if a powerful wipe tool has been used.

Issue 3: Lack of a backup or document retention policy

A document retention policy consists of the manner in which electronic documents are reviewed, retained, and destroyed throughout the course of normal business operations. Such a document retention policy should be based on state and federal statutes/rules that identify the length of time documents must be retained. The policy should also include steps for recording all documents that have been destroyed and should be updated as discovery obligations arise.

Issue 4: Not complying with preservation orders

Once a lawsuit is pending, it is the organization's obligation to immediately cease the destruction of electronic documents, as they may contain relevant evidence. It is crucial that the IT personnel responsible for such actions be informed of the preservation order, as they are often overlooked. In addition, any automated destruction systems must also be discontinued.

Issue 5: Failure to utilize certain forms of evidence

Electronic information is often stored on media devices that can be more difficult to work with, such as backup tapes, PDAs, or electronic tablets, and are often ignored. However, these forms of media often contain useful and relevant electronic evidence that can prove critical to the case. Many experts are able to work with these more difficult types of media, and retaining them early will help if the court orders production of electronic information contained within them.

Issue 6: Failure to produce all electronic evidence

The same rules apply for electronic evidence as they do for more traditional forms of evidence. The court system has broad discretion when applying sanctions for failing or waiting excessively to produce electronic evidence, including declaring a mistrial, delaying the start of the trial, imposing monetary penalties, or issuing an adverse inference instruction. Sanctions may be applied not only when a party has been grossly negligent or acted in bad faith, but also due to ordinary negligence.

Issue 7: Failure to forensically duplicate hard drives used by departing employees

Policies should be in place regarding the management of computer systems used by departing employees, both those that were terminated and those that resigned. In the event that litigation arises, the information stored on the forensic duplication of a hard drive could act as a smoking gun, especially if the employee has taken the computer system in question with him/her or if it has been reallocated to another employee.

Issue 8: Failure to use experienced computer forensic investigators

In all likelihood, the average IT professional, although good at his/her job, does not have the necessary knowledge or experience to properly conduct and manage a computer forensic investigation. IT professionals are very well-informed with regards to the organization, media types, software used, and data retention policies, all of which is important to a computer forensic investigation. However, it is best if IT professionals work with computer forensic investigators as, if not done properly with the correct tools and techniques, files stored on the computer system can be destroyed or date and timestamps can be changed, thus tainting the evidence stored within them. Therefore, experts in the field of computer forensics should be retained in order to ensure that evidence is properly collected and admissible in a court of law.