



The Evolving Legal Landscape of Electronic Discovery

It is estimated that over 90% of all documents are now created electronically, although most of them are never printed; therefore, legal professionals are being challenged by a drastic increase in electronic evidence. Legal professionals now must devise and execute a plan for handling electronic discovery, while also protecting their clients' interests and remaining strategically positioned ahead of their opponents.

Data Preservation

Initially preserving data is the most crucial step to electronic discovery. Organizations must protect themselves from a potential spoliation accusation by ceasing the destruction or recycling of backup tapes or other electronic data when litigation is pending or appears imminent. In addition, it is often useful to create mirror image duplications of hard drives utilized by key players in the case, and preservation letters should be sent to all parties or nonparties that may possess potentially pertinent information or a preservation order should be moved for. Monitoring compliance with these data preservation orders is important to undertake throughout the case.

Spoliation Concerns

Spoliation of electronic evidence is extremely easy to do and occurs most often when automatic electronic document destruction is not discontinued, electronic information is improperly gathered and imaged, or websites are modified. If information is not properly copied for production via sector by sector imaging or even if a computer system is turned on, slack and temporary files may be destroyed, resulting in spoliation. In addition, if a file is clicked on rather than copied, it can change the date it was last accessed, potentially causing the evidence to be deemed inadmissible.

Understanding the potential for spoliation to occur is crucial to not only protect clients but also when serving an interrogatory questioning whether the opposing party has overwritten or revised any relevant electronic documents since litigation began. In addition, if a motion to compel production is made and the information is produced in an altered form, it is possible that spoliation may have occurred. Parties possessing little electronic information or who have a clear understanding of their own electronic evidence often request large amounts of electronic evidence from opposing parties in an attempt to cause spoliation.

Sanctions imposed for spoliation can be severe and often include the declaration of a mistrial, a delayed start to the trial, monetary penalties, or an adverse inference instruction or presumption,

or can even result in a separate cause of action in tort. Criminal penalties relating to destruction of evidence can also be applied at the federal level.

Rule 26 Disclosures

Rule 26(a) calls for the full disclosure of data compilations, such as email messages, electronic files, and databases after an investigation has been completed. Therefore, legal professionals must have knowledge of all the electronic information their clients possess, including on desktops, laptops, disks, tapes, CD-ROMs, network hard disks, and PDAs, as well as any information possessed by third parties.

The amount of email and other electronic evidence must be identified under Rule 26, as this information can be vital to negotiations regarding the timing, form, and limitations on discovery. Rule 26(a) also mandates that any person who may be called to present evidence under Federal Rules of Evidence 702, 703, or 705 must be disclosed. This includes any expert that has been retained to perform forensic analysis on hard drives or other information technology systems, however, the rule does not specify whether an expert who only manages the collection and reproduction of electronic information without performing forensic analysis must also be disclosed.

Rule 16 Conferences

Rule 16's pretrial conference can be extremely helpful for managing electronic discovery, since important topics such as preservation of evidence, preliminary discovery regarding the opposing party's computer systems, document processing and production formats, testifying experts, and anticipated evidentiary disputes can all be discussed. As per Rule 26(f), legal professionals must possess the necessary information regarding all relevant electronic evidence, as being prepared may help limit the overall scope of discovery.

Discovery Requests and Review

By utilizing a combination of carefully crafted interrogatories, requests for documents, and depositions seeking to identify information applicable to the claims and defenses of the case, legal professionals may obtain additional information pertaining to electronic evidence. Useful interrogatories can be created based on the same criteria used to disclose information under Rule 26 and their response should provide a plan for additional document requests.

Many advantages and disadvantages exist with regards to electronic evidence. Although electronic documents are much easier to search through as opposed to hard copy documents, mistakes can be made due to the sheer number of electronic documents present in any organization. However, the discovery of a smoking gun in an electronic document can often result in settlement rather than proceeding with litigation.

Trial Issues

In the event that spoliation has not occurred and a smoking gun has not been identified, it is still possible for questions of admissibility of electronic evidence to arise at trial. In order to ensure that electronic evidence is found admissible, it must first be authenticated and found to not be hearsay, as computer documents are often admitted under the business records exception to the hearsay rule. To be recognized as an exception to the hearsay rule, the party entering the electronic document into evidence must be able to prove that it was in fact created at the time of the event in question.

As technology advances and is used more often in daily business activities, the use of electronic evidence in litigation is critical to a victorious outcome. In today's world, instead of being found in storage boxes, the most useful evidence is now often found in the computer systems utilized by the organization each day. Therefore, by possessing a clear understanding of the ways electronic discovery and evidence are used, legal professionals are better able to successfully assist their important clients.