Preservation Orders: Securing Electronic Evidence

Introduction

The increased dependence on technology-based methods of communication has impacted enterprise investigations and legal matters by requiring evidence created, stored, and accessed electronically to be considered. Computer forensics and electronic discovery have become critical in the identification of electronic evidence, its integration into case strategy, and in response to discovery requests for electronic information.

Electronic information is extremely mutable, as it can be easily accessed, produced, or changed, therefore, litigation involving electronic evidence must take into account electronic evidence preservation orders and legal professionals' ability to minimize the associated inconvenience, cost, and business disruption to their clients.

Preservation Orders

When choosing whether to enter a preservation order, a court can exercise broad discretion. Although generally inconvenient and possibly even crippling to the party required to preserve evidence, the courts often enter such orders regardless, sometimes on an ex parte basis. When determining whether such a preservation order should be entered, the courts generally look at the following three factors: 1) whether it can be demonstrated that relevant information will likely be destroyed if not protected, 2) whether irreparable harm will be caused if the order is not entered, and 3) the burden imposed if the order is granted.

1. Probability of Destruction or Corruption

The first and possibly most important factor considered by the court is whether it can be demonstrated that relevant information will likely be destroyed if the order is not entered. Since the opponent already has a duty to preserve all relevant evidence, the movant must establish and demonstrate that this duty is not being followed. Although it is easier to argue this factor when considering paper documents, it is much more difficult with electronic information as it is often configured to automatically delete and/or alter itself, especially when dynamic databases or websites are utilized.

2. Risk of irreparable damage

The court also must weigh whether irreparable harm will be caused to the movant if the order is not entered against the likelihood that the opponent is already doing its duty to preserve relevant evidence. As many organizations operate in a manner in which electronic information is continuously changed or deleted throughout the normal course of business operations, a movant will seek to utilize the alterable nature of electronic evidence to show that it will suffer

irreparable harm if the preservation order is not entered. In addition, the opposing party will likely argue that they are already preserving evidence based on the threat of sanctions being imposed if they were to ignore this duty, as well as inform the court of any back-up systems in place that store archived copies of electronic information.

3. Undue Hardship

Based on the third factor, the court must determine whether entering such an order would place an undue hardship on either party. While the movant will state that there is no additional hardship since there is already a duty to preserve evidence, it is important for the opponent to demonstrate that what may seem like a harmless preservation order, in actuality, disallowing an organization from changing or adjusting any electronic information can literally bring it to a standstill. Such an order would prevent the opponent from utilizing electronic information in its basic forms, such as updating customer databases, modifying web pages, imaging documents, or deleting any email messages, which would likely cause a major disruption to normal business operations.

Aside from disruption to business, it could be physically impossible to comply with such a preservation order in total, as one that includes all computer memory would be immediately violated since computer systems continually, repeatedly, and automatically delete data stored in their random access memory at their own volition. Complying with such a preservation order can also be extremely costly, as it may necessitate the implementation of monitoring systems, require extensive logs to be kept, or require additional employees or outside consultants or experts to be retained.

It is often necessary to oppose a preservation order in an attempt to remain free from a contempt hearing should any electronic evidence mistakenly be lost or destroyed during litigation. However, it may prove beneficial for both parties to willingly agree to a preservation order to denote the relevance of electronic information, define the scope of duties, or provide the court with a standard by which production efforts can be judged.

Defense of Preservation Orders

The following steps will help to minimize the potential disruption and costs associated with an electronic information preservation order:

A. Understand the client's Business and Technology

Communication with the clients involved in each case is essential to ensuring that disruptions and costs are minimized. It is important for legal professionals to obtain a thorough understanding of their clients' electronic and information systems and the roles they play in performing daily business activities. Before becoming entrenched in litigation, legal professionals should meet with the head of the IT department to gain an understanding of the computer systems, backup systems, and storage procedures utilized by the organization, as well as determine the value of electronic information to the total business.

Although vital to the course of litigation, when presented with a preservation order legal professionals should not rely solely on the information gained during these meetings. Instead, the client should be consulted to obtain the necessary information so injunctive factors can be argued and affidavits or testimony can be entered.

B. Pursue the Path of Least Resistance

When it appears that the court is predisposed to granting a preservation order, changing the focus away from complete defense to seeking the least restrictive language from the court, as well as a specific scope to the order, should assist with compliance abilities. Less restrictive language and a clearly delineated scope will likely allow the client to actually comply with the order with fewer restrictions to normal business operations.

Specifically, limiting the scope to only key company networks and mainframes, rather than all laptop computers and PDAs, will make compliance much more attainable, since it would be extremely difficult for a large organization to secure these devices from possibly thousands of employees. In addition, an exception for actions taken throughout the course of normal business operations should be argued for, as well as a "reasonable steps" or "best efforts" clause in the preservation order. Such a clause would provide protection against sanctions imposed for innocent or unintentional violations, as compliance with such orders can be extremely difficult.

Conclusion

When organizations are compelled to comply with preservation orders, it often causes disturbance, frustration, and high costs, or even brings normal business operations to a standstill. Therefore, it is important to understand how dependant organizations are on their computer operations. Utilizing this knowledge, important issues pertaining to electronic evidence preservation orders can be more easily addressed.