



Portfolio Media. Inc. | 860 Broadway, 6th Floor | New York, NY 10003 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

Think Before You Delete: Spoliation And E-Discovery

Law360, New York (October 31, 2011, 12:08 PM ET) -- In a world where emails, text messages and voicemails have nearly replaced letters, the litigation discovery process is no longer as easy as simply opening up a file cabinet and copying all the documents that may relate to the claims in a lawsuit. Over the last several years, both lawmakers and courts have begun serious efforts to create laws that corral the "spoliation" (or destruction, alteration or failure to preserve evidence) of electronically stored information (commonly referred to as "ESI").

Courts are now sanctioning parties who not only willfully destroy potentially relevant evidence, but also those who have simply failed to take any practical steps to ensure that ESI is not altered, modified or destroyed once a litigation is reasonably likely to occur, or who have failed to conduct a meaningful investigation to identify, preserve and collect any materials that may be related to a law suit.

However, there is no consensus among either state or federal courts as to what steps need to be taken to avoid sanctions for spoliation of ESI. At this time, what can be concluded, based on the current cases, is that the best way for companies and organizations to abide the new ESI rules is to act proactively by implementing, well in advance of threatened litigation, a "preservation policy" that directs "key persons" (i.e., anyone who it believes may have records in connection with the matter) to preserve all relevant data in the event litigation is commenced.

Even more, it is not enough to simply have a "preservation policy" to prevent the spoliation of potential evidence, but courts may now examine the policy to make sure that it is comprehensive enough to cover all areas where potential evidence may be stored and that it contains a mechanism by which identified materials will be collected and preserved.

ESI Preservation Guidelines and Recommendations

In 2006, Congress amended the Federal Rules of Civil Procedure to address specifically the preservation of ESI. Similarly, in June 2009, the California legislature enacted the Electronic Discovery Act ("EDA"). The EDA essentially amended the California Civil Discovery Act to cover records that are "electronic," which is defined as "relating to technology having electrical, digital, magnetic, wireless, optical, electromagnetic, or similar capabilities," as well as to cover "electronically stored information," which is defined as "information that is stored in an electronic medium."

The goal of these amendments both at the federal and state level is the same, namely ensuring litigants avoid attempting to obtain an advantage in litigation by destroying, altering or withholding evidence related to a case regardless if that evidence is kept in a file cabinet or on a hard drive. The net effect of both these laws requires every business to implement a "preservation policy" that directs "key persons" (i.e., anyone who it believes may have records in connection

with the matter) to preserve all relevant data and create a mechanism to collect it.

While the EDA is relatively new, based on cases discussing the ESI amendments to the Federal Rules of Civil Procedure, the type of conduct the EDA could encompass includes not just the willful destruction and or alteration of records but also simply failing to preserve records once a party is engaged in a dispute that could lead to a potential lawsuit.

Under both federal and state law, a court may impose several different types of sanctions for a failure to preserve all records in connection with a lawsuit. These sanctions can include:

- Monetary sanctions against a party and/or its attorney;
- Issue sanctions in which the court will issue an order designating that certain facts are deemed established in favor of the party adversely affected by the abuse of discovery;
- Evidence sanctions meaning that the court can issue an order prohibiting certain information from being introduced into evidence at the trial; or
- Terminating sanctions (e.g., dismissing a plaintiff's complaint or entering a judgment against the defendant)

Traditionally, at both the federal and state level, trial courts have broad discretionary power to impose discovery sanctions. Thus, the type of sanction a court may impose depends on the judge's assessment of the conduct. However, there is no consistency between the courts at either the state or federal level as to what conduct a court may sanction, and because of this there is no clear, concise list of what a company can and cannot do in connection with ESI once it has notice of even a potential lawsuit.

For example, there have been cases that sanction a party for mere carelessness (e.g., permitting servers to be replaced while litigation is pending) to cases that sanction a party for gross misconduct (e.g., destroying a laptop that the person knew contained emails relevant to the lawsuit).

Based on the lack of a bright-line test in this area, we recommend our clients proceed in the manner specified by the Judge Paul W. Grimm of the United States District Court in Maryland in a decision published in September 2010 (Victor Stanley Inc. v. Creative Pipe Inc. et al, Civ. No. MJG-06-2662 (Sept. 9, 2010)): "The only 'safe' way to do so [implement a preservation policy] is to design one that complies with the most demanding requirements of the toughest court to have spoke on the issue, despite the fact that the highest standard may impose burdens and expenses that are far greater than what is required in most other jurisdictions in which they do business or conduct activities."

Heeding Judge Grimm's advice, when faced with potentially commencing or defending a lawsuit, we advise our clients immediately do the following:

- 1) Identify the "key persons" who may have information about the matter. A key person essentially is any employee, officer, agent or consultant who may have data in connection with the matter. This would include any person who may have worked on this matter in any manner at any time.
- 2) Once the key persons have been identified, the business should deliver to each of them a "litigation hold" letter directing them to search and preserve (i.e., not delete, alter or modify) all materials (electronic and hard documents) they may have in their possession that relate in any way to the matter (without the person making any determination as to what is factually or legally

relevant).

The business must explain that the search for these materials includes documents in tangible format as well as computer files, emails, electronic calendars and even text messages. Further, the search of emails must include those in the person's "inbox" as well as "sent" and "deleted" emails. This litigation hold letter must also provide clear, easy-to-follow instruction on how to preserve the ESI once it is located so it can be collected and reviewed by counsel. In addition, the litigation hold letter should provide contact information for technical assistance for this process.

3) Contact the IT department (or IT consultants) to inform them of the matter and instruct them that no computers of any of the key persons are to be altered or modified in any way and that all back-up procedures that may override or delete dates on the servers is to be suspended until further notice. A copy of the litigation hold letter should also be sent to them.

While the business should take the above steps as soon it contemplates bringing a lawsuit or learning it will be defending one, we also recommend that business do the following to devise a preservation policy:

- In-house counsel and/or senior executives in charge of litigation must become familiar with the business's ESI back-up procedures. It is imperative to know how often ESI is deleted from the company's servers and how those procedures can be suspended once a lawsuit has been threatened so that backed-up files are not inadvertently deleted. It is no longer acceptable to tell courts that evidence was lost because the person at the business in charge of the litigation was not aware that back-up data was regularly destroyed and no steps were taken to preserve it.
- Implement procedures in the employee handbook that prohibit employees from altering the hard drives on their computers without the approval from in-house counsel or senior management. Further, employees should be directed that they are not to install software on their computers such as "Easy Cleaner" or "CC Cleaner" that "scrub" or delete data from not only their computers but the servers as well.
- Adopt and consistently implement a preservation policy that not only defines a document-retention decision-making process, but also establishes procedures for the reporting of information relating to a potential threat of litigation to a responsible decision maker.

Document all steps that have been taken to preserve ESI. Once litigation commences, it could easily be months to over a year before the business may be asked about what preservation steps it has taken, and memories can easily fade by then or employees who were handling the process may have left the company's employ. However, if all the steps are documented in writing, then the business should be easily able to substantiate the preservation steps it took either to its adversary or to the court.

--By Tricia L. Legittino, Frandzel Robins Bloom & Csato LC

Tricia Legittino is an attorney with Frandzel in Los Angeles.

The opinions expressed are those of the author and do not necessarily reflect the views of the firm, its clients, or Portfolio Media, publisher of Law360. This article is for general information purposes and is not intended to be and should not be taken as legal advice.

All Content © 2003-2010, Portfolio Media, Inc.