

# IGNORE THIS AT YOUR PERIL!

By Luis S. Konski,  
Fowler Rodriguez Valdes-Fauli

Now that I have your attention, be aware that there has been a sea-change in how litigation discovery and internal corporate investigations are taking place.

This article is not to delve in detail on what you as corporate management or as in-house counsel should be doing to preserve electronically stored information (“ESI”). The purpose is to inform you that failure to do so is an unnecessary assumption of risk.

Literally, there is a tsunami of electronic information waiting to swamp all but the most elementary of cases. Management, in-house counsel and information technology professionals will have to learn to communicate and coordinate efforts or you will lose your cases not because of the merits of the case, but because you failed to preserve electronic evidence.

Recent court decisions point to the wave of the future. Learn to surf or you will be swamped.



Once upon a time, all we worried about in trying a case was making sure that all relevant and non-privileged paper documents were provided and received within the bounds of discovery. We would use a simple sequential numbering machine like a Bates™ stamping machine to keep an accounting of what relevant documents are being provided or held back because of privilege. That was history. History is not always prologue.

Now, unless you control the electronic documents that may be relevant and prevent their inadvertent disposal, you, as management, and your lawyers may be held liable, regardless of the merits of the case.

Sanctions have involved millions of dollars and a judgment against the offending party. You may lose by default.

### ***CASE IN POINT.***

Recently, a former CEO sued my client's corporation for 4.9 million dollars in damages for his having been wrongfully terminated. The corporation was a nascent technology firm. Immediately, I asked my client to mirror-image (an exact electronic copy of) all his company's stored electronic information, and to provide it to me. At the same time I informed the CEO's counsel, a former U.S. Attorney who was a partner of a nationally renowned firm in Miami that he needed to advise his client to preserve all electronic evidence, and return a laptop computer belonging to the corporation. Unfortunately for the plaintiff, my requests were ignored.

Eventually, upon my motion the Court entered an order requiring that all parties preserve electronic evidence, and after extensive motion practice the judge agreed that while the ownership of the laptop computer may be considered at a later time, the laptop computer would be turned over to an independent forensic computer

expert to review the hard drive and retrieve corporate documents.

The forensic expert reviewed the laptop's hard drive and discovered that the former CEO, a lawyer, installed a program whose name was Evidence Eliminator™. It was also discovered that the program was installed on the eve of the Court's preservation order, and that plaintiff used the program to remove some of the files from the computer.

Although the file-scrubbing software was thorough in obliterating the contents of the selected files, the equivalent of "electronic fingerprints" were left behind. The original names of at least some of the removed files remained, although the files were irretrievable and overwritten.

Under oath, the former CEO claimed that none of the documents removed were corporate documents or relevant to the litigation. Through detective work I was able to determine that some of the files removed were corporate documents and highly relevant to the litigation. (How I did that is another story.)

Facing a deposition on his destruction of evidence, the former CEO dismissed the suit. However,

we objected and ultimately took the deposition the CEO tried to avoid. During the deposition it became clear that the former CEO had destroyed highly relevant evidence using Evidence Eliminator. Some of the evidence showed that he, along with other fiduciaries of the corporation, had engaged in a conspiracy to take over the corporation. It was clear that this is what the CEO tried to hide.

Soon after, without our being required to file a countersuit, the former CEO asked for mediation and ultimately paid the corporation \$300,000.00 to avoid a hearing on sanctions for destruction of electronic evidence.

Although we had good substantive defenses against the CEO and counterclaims, it did not matter. My opposition lost, early on the case, literally with my first letter, because they failed to recognize, from the get-go that electronic evidence and its preservation was the key to the case. Arrogance was the former CEO's undoing. Let this not be you. Be assured, there are ways to avoid the same outcome.

## *READY TO DIVE OFF THE CLIFF?*



The key moral here is you either evolve or perish. Corporate records are estimated to comprise 98 percent of the records of any given corporation. The problem is: How do you as a manager, in-house counsel or information technology professional preserve those documents you will need to prosecute of defend cases? The risks are substantial. Destruction of evidence whether inadvertent or intentional can mean your case

First, let's talk about culture and what I call corporate anthropology. Corporations, of course, are made up of people. People have different drives and in particular, different professions have different worldviews. Preservation of evidence requires interaction of three different functions with different strengths and different outlooks.

Management is mostly interested in managing the firm and bringing in the income while keeping expenses down. The information technology professionals are interested in running the computer system and finding storage space for old electronic information. In-house counsel is primarily interested in making sure that legal issues are dealt with and anticipated.

The question is how to make certain that with these disparate perspectives, often with colliding imperatives, communicate to make certain that electronic evidence is preserved and accessible for potential litigation or investigations. This is where a forensic team, including outside counsel, who are conversant with the legal requirements of ESI, are needed.

### ***WHAT IS THE STANDARD?***

The obligation to preserve evidence attaches whenever there is a reasonable expectation that a matter may result in litigation. Translated, if there is any whiff you will sue or be sued and you destroy evidence that may be relevant you are in **BIG** trouble. Data is constantly overwritten as a routine business

practice. Any delay in taking preservation steps may increase the danger of claims that relevant evidence was not preserved.

Time is of the essence in handling ESI discovery projects. Not only is electronic data can be thoroughly evanescent, but according to the federal rules of procedure you have to be ready to hand over ESI evidence within 100 days of the filing of the suit.

It is important that you assess the data storage methods during the entire lifecycle of ESI and develop policies and guidelines for preservation of evidence. When litigation or an investigation is imminent a reassessment must be made of the data storage methods and the risks those methods may have. Then, an ESI discovery response plan needs to be created. Litigation hold notices have to go out, sources of ESI must be identified, ESI destruction must be suspended, methods of collecting and preserving ESI must be implemented, and a procedure must be instituted to determine whether the ESI is relevant or privileged, and if the latter, a privilege log must be provided while

preserving the privileged communication.

### ***CONCLUSION***

Here is a summary of the headaches of e-discovery: The costs to preserve, find and review electronic evidence, including e-mails is astronomical. Mistakes in e-discovery are ubiquitous and may force the settlement of a case based on e-discovery and not the merits. ESI is easy to destroy or alter. The amount of electronic evidence stored by corporations is overwhelming. Computer systems and information storage have become so complex that any one expert may not understand it all. Most companies do not have functional ESI management policies. Many judges no longer accept the “empty head and pure heart” defense to ESI mistakes. The new federal rules accelerate the need to provide ESI at the beginning of the case, even possibly before the pleadings are finalized. Most lawyers and law firms are unprepared for e-discovery. And, most corporations and in-house counsel are unprepared for preservation of electronic evidence. This is a cocktail for disaster.

Our task group looks forward to discussing least-cost remedies to these technological conundrums. Ignore this at your peril.

*Mr. Konski is a partner with the law firm of Fowler Rodriguez Valdes-Fauli and a member of the firm's ESI Task Force. He would like to thank his colleagues and fellow members of this task force, Mary Isabel Hoelle, Partner, and Frank Quesada, Associate, for their assistance in preparing this article. Mr. Konski has been involved in electronic discovery since 1978.*

© 2008, Luis S. Konski