

CyberBytes™

Straight Talk about Electronic Evidence Discovery in Civil Cases- March 2006

E-Discovery Collaboration

Whether your clients are facing regulatory compliance, litigation holds or internal investigations, the steps of identifying, preserving, collecting, processing, reviewing and disclosing information is different. Understanding concepts such as "native file format," "metadata" and "residual data" and others will have to become part of your discovery protocol.

More importantly, this transition to handling the huge volume of electronic evidence requires timely collaborative action. In two leading discovery cases, we see the failure of collaborative action between in house counsel, outside counsel, IT personnel, witnesses, etc., resulting in severe court imposed sanctions. In both the Zubulake and Morgan Stanley cases, the failure to preserve and disclose electronic discovery resulted

in an adverse and a burden of proof inference instruction that resulted in a 29 million dollar employment case and a 1.4 billion dollar commercial case verdicts.

Was this lack of timely collaboration unusual? Maybe not, one survey has noted that 75 percent of AmLaw 200 law firms were not able to handle complex EDD matters (EDDix, LLC Survey, Sept. 2004). In fact, the courts have increased the risks to practitioners themselves by suggesting that failure to preserve and disclose "finds expression not only in the rules of discovery, but also in this Court's Rules of Professional Conduct, which prohibit an attorney from suppressing any evidence that the lawyer or client has a legal obligation to reveal or produce ..." (Danis v. USN Communications, Inc., 2000 WL 1694325 (N.D. Ill. Oct. 20, 2000)). This coupled with malpractice risks for not properly advising your clients re electronic

evidence can lead to devastating firm wide consequences.

No longer can counsel sit back after notifying their clients about a preservation mandate and assume their clients are fulfilling their discovery obligations. Instead, as expressed in several leading federal discovery cases, the courts have imposed mandates requiring outside and in-house counsel, IT personnel, witnesses, and other stakeholders to timely collaborate on discovery. As a result, counsel and their clients and electronic discovery specialists have to re-engineer the discovery and production process to prevent the management and cost risks in handling electronic discovery. This simply requires a new way of thinking and immediate change on the part of companies and other stakeholders.

At a minimum, it is necessary to develop a set of

litigation hold or regulatory compliance best practices focused on legal obligations, technology advancements and a commitment to work together. In an unprecedented fashion, the courts in several federal decisions have set forth in surprising detail discovery and compliance obligations for legal counsel. These obligations call for development of best practice protocols to ensure the preservation and disclosure of electronic evidence. These past decisions and future mandates have to be woven together with a corporation's document retention policies to ensure preservation and avoid spoliation charges. With paper discovery, one could compartmentalize the requisite identification, preservation and other production steps. Not so with electronic evidence, all of the stakeholders must be part of the procedural and substantive answer to data preservation. This will ensure that you have a "legally defensible collection".

Without changing your methodology of handing evidence, it is highly unlikely that your firm or

clients will survive this transition.

It is within this complex arena of electronic discovery and production that CyberControls' professional litigation support specialists and digital forensics practitioners are prepared to assist legal professionals and their firms.

To learn more about CyberControls and the digital forensic services and pre-trial litigation consultancy support, please call us at 847-756-4890 or visit our cyber sites at www.cybercontrols.net. You are also invited to write to us at cyberinfo@cybercontrols.net.

Robert Guinaugh

Editor. Robert Guinaugh

Contributors. Wolfgang Wilke

This document is neither designed nor intended to provide legal or other professional advice but is intended merely to be a starting point for research and information on the subject of electronic evidence discovery. While every attempt has been made to ensure accuracy of this information, no responsibility can be accepted for errors or omissions.

CyberBytes is a monthly newsletter published by CyberControls, LLC and

all contents are copyrighted with all rights reserved. Please submit your requests for distribution and additional copies to cyberinfo@cybercontrols.net
847-756-4890-Office
847-620-2500-Fax