

# CyberBytes™

## *Straight Talk about Electronic Evidence Discovery in Civil Cases- June 2006*

### When E-Production Simply Doesn't Cut It

It is common practice to expect that the majority of responding parties will conduct an adequate discovery effort in identifying, recovering, and review for all relevant and responsive materials to sufficiently comply with an evidence production request. In part, this affirmative perspective may be nothing more than a professional courtesy and mutual respect commonly shared by opposing counselors. Or, perhaps the requesting party feels confident that his/her electronic discovery request is so masterfully constructed, that the producing party could not possibly overlook any document, e-mail, e-mail attachment, and other relevant materials pertaining to the case in their resulting production. For a majority of requesting parties, the quality and quantity of the responsive

materials is often severely lacking in usefulness. It can be argued that pertinent, electronic evidence is in actuality, scarce.

In reality, the entire discovery process conducted by the producing party is rarely questioned, if at all challenged. Instead, we often see the requesting party trying to argue that the mere absence of substantive production materials is in itself a clear indication that the responding party has failed to adequately search for all relevant evidence. Without assuming a more pronounced, adversarial role in asserting input into the scope of the e-discovery process and methodology, the requesting party is likely to be disappointed with the results.

#### **Issues to be considered are:**

1. What formal policies and procedures were in effect at the time of the complaint

"events" at the producing party's place of business as it relates to e-documents, e-mails, and other forms of electronic records preservation and destruction? As a follow-up to that question; what if any specific changes have been adopted by the litigant since that time to the present?

2. Be prepared to outline with great specificity each of the areas of electronic data storage that you will require assurances from your opponent that the producing party will implement to prevent inadvertent spoliation of all relevant electronic information pertaining to the case and named litigants. A request for a written preservation protocol will be the appropriate approach to ensure that opposing counsel is engaged on this matter.

3. As part of the preservation of evidence stance, it is presupposed that you have intentions to

stipulate in your forthcoming e-discovery request, the specific states in which the evidentiary discovery and production will be conducted e.g., "active" data files and "inactive" (deleted) data files. By omitting deleted data files, the producing party will assume they have dodged a bullet, and no evidence of a deleted nature will be produced.

4. Get prepared in formulating the argument and plan to demand direct input into the search and recovery of relevant evidence of the responding party's computer systems e.g. identify specific computers, servers, and back-up systems where the search will be directed. Also, it is advisable to insist upon having input into the development of the search criteria to be used by the responding party to identify all responsive materials. If this involvement is vigorously resisted, at the very least, insist upon full disclosure of all search criteria to be used by any third-party service provider, and litigation attorneys to understand the depth of the search for pertinent evidence.

For some additional insight into the fast changing landscape of e-discovery options and considerations, you can download the white paper "Quantifying Digital Forensics Discovery Benefits" by clicking the link at the bottom of this message.

There are a number of other tactics available to complete in order to maintain an effective outcome to your e-discovery requests, which we at CyberControls are prepared to share with you and your litigation team. Please call us at 847-756-4890 or visit our cyber sites at [www.cybercontrols.net](http://www.cybercontrols.net). You are also invited to write to us at [cyberinfo@cybercontrols.net](mailto:cyberinfo@cybercontrols.net).

-----  
-----  
---  
To download the white paper "Quantifying Digital Forensics Discovery Benefits":  
<http://www.cybercontrols.net/common/downloaddoc.asp?docid=1642&id=93895>

*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](mailto:cyberinfo@cybercontrols.net)  
847-756-4890-Office  
847-620-2500-Fax