DIRECT INSPECTION
OF OPPONENTS' COMPUTERS

In the rapidly evolving law of electronic discovery, the degree of the intrusiveness of e-discovery demands is a key consideration. Many litigants seeking discovery demand direct access to the computers and computer systems of their adversaries. These demands may be based on evidence that the responding parties have failed to comply with their e-discovery obligations. Such demands rest on the concept that the demanding parties need direct access to their opponents’ computer systems in order to retrieve information that their opponents refuse to produce.

However, more aggressive litigants may attempt to obtain direct access without showing e-discovery misconduct by their opponents. Instead, they may base such demands on their opponents' mere failure to produce certain categories of responsive electronically stored information, or on an unsubstantiated suspicion that their opponents may have deleted such information or rendered it inaccessible.

Courts are resisting such demands for direct inspection of opposing parties' computers that lack a foundation of e-discovery misconduct by the opposing parties. A key recent example is the decision in Powers v. Thomas M. Cooley Law School, 2006 WL 2711512 (W.D. Mich. Sept. 21, 2006). In Powers, the plaintiff claimed that she had been denied accommodations to which she was entitled as a consequence of a visual disability. Her case rested in part on the assertion that the computer systems provided by the law school for the use of visually disabled persons repeatedly malfunctioned.

During discovery, the plaintiff contended that the law school had failed to obey a prior court order requiring it to produce all work orders relating to the allegedly malfunctioning computers, and moved to compel compliance. The law school put on evidence that it had previously produced responsive work orders in hard copy, and that the replacement of its work order system with a new system had rendered it impossible to retrieve work orders in electronic form that had been generated under the old system. At this point, the plaintiff's counsel made an oral motion that her expert be allowed to conduct a forensic search of the law school’s computers to extract information from the old work order system.
The court entertained but denied the plaintiff’s oral motion, and denied a subsequent motion for reconsideration. The amendments to Federal Rule of Civil Procedure 34 effective December 1, 2006 authorize testing or sampling of an adversary’s computers, but also admonish in the advisory committee notes that the amendments were "not meant to create a routine right of direct access to a party's electronic information system." As the Powers court put it, "direct inspection of an opponent's computer should be the exception and not the rule." Since the sole foundation for the plaintiff’s direct access demand in Powers was her "mere suspicion that the opposing party may be withholding discoverable information," there was no basis to apply the exception and allow direct access.

In reaching this result, the court also observed that the discovery process "relies upon the responding party to search his records to produce the requested data." In the absence of a strong showing that the responding party has failed to perform that duty, courts should not resort to "extreme, expensive or extraordinary means" — such as forensic examination of computer hard drives — to guaranty compliance.

Demanding parties need to take heed of this hurdle. Any demand for direct forensic inspection must have proper evidentiary foundation supporting the conclusion that the responding party has failed to comply with the duty to preserve and produce responsive electronically stored information.

On the other hand, responding parties need to document in detail their compliance with e-discovery requests, and must be in a position to explain how and why any responsive information they fail to produce no longer exists or is no longer reasonably accessible. Indeed, changes to computer systems like the one made by the law school in Powers can be a trap for the unwary. Under revised Federal Rule of Civil Procedure 37(f), a responding party who – after litigation becomes reasonably foreseeable – deletes potentially responsive electronically stored information or renders it inaccessible may not qualify for Rule 37(f)’s "safe harbor" against e-discovery sanctions, and may be subject to an array of monetary, evidentiary and even preclusionary sanctions.
Direct Inspection Of Opponents' Computers

Contact:

Stanley M. Gibson
310.201.3548 • mailto:SGibson@jmbm.com

Dan P. Sedor
310.201.3554 • mailto:DSedor@jmbm.com

Michael A. Gold
310.201.3529 • mailto:MGold@jmbm.com

Robert E. Braun
310.785.5331 • mailto:RBraun@jmbm.com

©2006, Jeffer, Mangels, Butler & Marmaro LLP