

# CyberBytes™

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

## Misappropriation of Trade Secrets

In early August, 2006, an interesting case, Lockheed v. Speed, came before U.S. District Court, Middle District of Florida, upon the Motion to Dismiss by the defendants. Lockheed alleged that three former employees violated the Computer Fraud and Abuse Act ("CFAA") by accessing Lockheed computers, copying proprietary information from them and delivering trade secrets to the Defendant L-3 Communications Corp. (L-3).

Lockheed alleged that L-3, in an effort to gain an unfair advantage for a government contract bid, conspired with three Lockheed employees to wrongfully obtain Lockheed trade secrets that pertained to the Plaintiff's bid response.

Lockheed submitted mountains of computer forensic evidence that substantiated that each of the three former employees accessed and copied hundreds of confidential and proprietary information data files and trade secret protected information of a specific nature having to deal with the ATAR I project. This wholesale copying of electronic information

onto compact disks was carried out right up to the final day of the defendant's departure from Lockheed.

Based on these allegations relating to the former employees, Lockheed asserted to the Court that it had federal jurisdiction over the matter pursuant to the CFAA.

For the sake of brevity, Lockheed's most significant allegation addressed the Defendants' violation of §1030(a)(4) of the CFAA which provides that whoever "knowingly and with intent to defraud, accesses a protected computer without authorization, or exceeds authorized access, and by means of such conduct furthers the intended fraud and obtains anything of value, unless the object of the fraud and the thing obtained consists only of the use of the computer and the value of such is not more than \$5,000 in any 1-year period".

The Defendants assert that they did not "access without authorization" or "exceed [] authorized access" in violation of the statute because Lockheed permitted the Employees,

as a function of their respective positions, to access the precise information at issue. Lockheed countered by arguing that "the authority of an agent terminates if, without knowledge of the principal, he acquires adverse interest or if he is otherwise guilty of a serious breach of loyalty to the principal." Because the Employees accessed information with intent to steal and deliver to a competitor, Lockheed argues, the Employees acquired adverse interests, terminated their agency authority, and therefore accessed "without authorization."

The term "without authorization," is not defined by the CFAA. Nonetheless, "authorization" is commonly understood as "[t]he act of conferring authority; permission." On the other hand, the CFAA defines "exceeds authorized access" as follows: "to access a computer with authorization and to use such access to obtain or alter information in the computer that the accesser is not entitled so to obtain or alter [.]

The Court granted the motion to dismiss by applying the plain meaning of the statutory terms to the facts of

the case, it is clear that the Employees accessed with authorization, did not exceed their authorization, and thus did not violate §1030(a)(4). Because Lockheed permitted the Employees to access the precise information at issue, the Employees did not exceed authorized access. Further, the Court opined that §1030(a)(4) does not reach the alleged subsequent actions of the Employees in their willful dissemination of any proprietary information to their new employer L-3.

CyberControls is a professional services provider specializing in computer forensics and pretrial litigation support in the area of electronic discovery. We welcome the opportunity to discuss any specific issues that you may be facing as a respondent or requesting party in a commercial litigation matter at 847-756-4890 or visit our cyber site at [www.cybercontrols.net](http://www.cybercontrols.net). You are also invited to write to us at [cyberinfo@cybercontrols.net](mailto: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](mailto:cyberinfo@cybercontrols.net)  
847-756-4890-Office 847-620-2500-Fax