"Authorization" and "Access" in the Computer Fraud and Abuse Act

03.15.2010

Berkeley HeartLab, Inc. (BHL) has filed suit in the Eastern District of Virginia against Health Diagnostic Laboratory, Inc. (HDL) and several former BHL employees for theft of trade secrets, breach of contract, and several other causes of action. The breach of contract claims refer to a Proprietary Information and Invention Agreement between BHL and the former employees, who allegedly left BHL en masse to work for Richmond based HDL. The Complaint also includes a claim under the Computer Fraud and Abuse Act, 18 USC 1030 (CFAA).

The CFAA protects against unauthorized access or hacking into to certain computers or information. For example, the knowing access of a computer without authorization (or exceeding authorized access) for obtaining certain types of information and willfully providing it to someone who is not authorized to receive it is a crime. Much of the buzz over the CFAA has been with the sensational criminal case United States v. Drew, over cyber-bullying.

However, the CFAA also provides a civil claim for some types of prohibited conduct:

> (g) Any person who suffers damage or loss by reason of a violation of this section may maintain a civil action against the violator to obtain compensatory damages and injunctive relief or other equitable relief. A civil action for a violation of this section may be brought only if the conduct involves 1 of the factors set forth in clause (i), (ii), (iii), (iv), or (v) of subsection (a)(5)(B). Damages for a violation involving only conduct described in subsection (a)(5)(B)(i) are limited to economic damages. No action may be brought under this subsection unless such action is begun within 2 years of the date of the act complained of or the date of the discovery of the damage. No action may be brought under this subsection for the negligent design or manufacture of computer hardware, computer software, or firmware.

18 U.S.C. § 1030(g). Some employers have brought CFAA civil claims against employees that have misappropriated information; the CFAA offers a federal remedy that does not involve the burden of proving that the information stolen was a trade secret.

For example, the BHL Complaint characterizes BHL computers as “protected computers” used in interstate commerce (citing 18 U.S.C. § 1030(e)(2)(B)), and that the former employees “accessed BHL’s computers

without authorization and, as a result of such access, made unauthorized copies of computer data." Complaint, ¶ 174. The Complaint spells out a number of factors that BHL might use to argue that it defined and controlled authorized access for
its employees, such as using "key-coded access," "password protecting patient and sales information," and controlling sensitive information. Complaint, ¶¶ 23 - 27.

A brewing conflict in civil CFAA litigation dwells specifically on the meaning of the statutory words: "authorization" and "access." There is a split between the seventh and ninth circuits on proving these terms. A background of the cases defining the split may be found at the blog for the Journal of Intellectual Property Law & Practice. Without repeating the background provided there, in short, the Seventh Circuit reasons that authorization for access to an employer's computer terminates at the time an employee breaches the duty of loyalty to the employer. The Ninth Circuit requires a more specific showing of how the employer defined authorized access for the employee, including its safeguards for sensitive information.

BHL's suit now brings the question to Virginia, and may reveal if the Eastern District of Virginia will choose to follow one of the existing standards, or decide to go its own way.

UPDATE: This case was settled, and dismissed per order of the Court on April 22, 2010.

Related People