February 19, 2013

InsideCounsel.com

BUSINESS INSIGHTS FOR LAW DEPARTMENT LEADERS

IP: Why companies need clear policies against giving computer access to non-employees

A well-established practice of restricting access can increase the chances of a successful Computer Fraud and Abuse Act claim

BY HON. JAMES WARE (RET.) AND MINDY L. WARE

In 1986, in recognition of the economic importance of protecting computers from unauthorized access, Congress passed the Computer Fraud and Abuse Act (CFAA). The CFAA imposes criminal liability on outsiders who access computers to steal information or to disrupt or destroy computer functionality. In 1994, the CFAA was amended to give computer owners the right to bring a civil action, which requires proof that a company has policies and practices that restrict access.

In general, there are three types of unauthorized access of concern to companies:

1. A non-employee (a hacker) may trespass into the system.

2. An employee may access a restricted zone or use information from a permissible zone in an impermissible manner, known as a "user exceeding authorization."

3. An unauthorized user may give access to an authorized user, known as a "permissive intrusion."

Although a clear company policy restricting access is important with respect to each of these, it is especially significant with respect to the third—namely, a case of "permissive intrusion"—insofar as the absence of such a policy might prove fatal to a CFAA claim.

Examples of permissive intrusion are all too easy to imagine. For instance, an employee who is traveling may need information that is on the company server, but may be unable to access the server via the Internet from his location. In such a situation, the employee might call his wife and provide her with his password, asking her to log in to his account. Alternatively, a company might provide a network password to a vendor, allowing the vendor to obtain needed specifications. Although these uses seem perfectly innocent, problems could arise if this permissive access can harm the company. In that case, the company would have to prove that the access, though permissive, was not authorized within the meaning of the CFAA.

The situation is made all the more confusing because the CFAA does not provide a definition of the phrase "without authorization." The 9th Circuit has held that "a person uses a computer 'without authorization' . . . when the person has not received permission to use the computer for any purpose . . . or when the employer has rescinded permission to access the computer and the defendant uses the computer anyway." Whether this definition also applies to the third type of unauthorized access—the "permissive intruders"—requires us to consider the law of agency.

Generally, an agency relationship exists when one person contracts to act on behalf of another. Thus, when an employee receives access to a computer to further the interests of his employer, the employee is an agent of the employer. The law of agency treats an act of an agent as "unauthorized" if it is beyond the express, implied or apparent authority of the agent. Thus, the company should set forth a clear policy regarding the authority of its employees to give access to company computers. Such a policy should be included in each employee's employment contract. Then, if an employee gives another person access to company computers in violation or in excess of what company policy allows, that employee would be regarded as acting outside of the scope of his agency. In that case, the element of "unauthorized access" of the CFAA would be satisfied, because access that an employee gives to an intruder outside of the scope of agency would render the authorization invalid under the general law of agency.

Although the CFAA and its interpretation pose a number of legal issues, this discussion underscores the importance of one simple rule: Companies should have a clearly stated, consistently enforced policy prohibiting authorized users from giving access to third parties for any reason whatsoever.

Judge James Ware (Ret.) is a full-time arbitrator and mediator with JAMS. Prior to joining JAMS he spent sixteen years as a civil litigator, and twenty-four years as a judge. He can be reached at jware@jamsadr.com.

Mindy L. Ware is an attorney and lecturer in the Liberal and Civic Studies Program at Saint Mary's College of California.