

# Law Trends

A Publication by Eastman & Smith Ltd.

Attorneys at Law since 1844

July 2007

## University Allowed Use Of A Warrantless Search

By Amy J. Borman



To protect its information systems from disruption, when can a university protect its network through a remote search without a warrant? A network administrator of Qualcomm Corporation discovered that someone at the University of Wisconsin (Madison) had hacked into the company's computer network. He contacted the FBI, as well as a network administrator at the University of Wisconsin (Jeff Savoy).

Savoy found that a certain computer had hacked *both* into the Qualcomm computer network *and* the University of Wisconsin network. In the course of his investigation, he discovered the IP address of the computer, and found that the computer at that IP address had been used to exclusively and repeatedly check the email of a student named Heckenkamp. Heckenkamp was a computer science graduate student who had a history of gaining unauthorized access to secure sites. Savoy was afraid that Heckenkamp could use his technical expertise to disrupt the university email system, so he electronically blocked the connection between the suspect IP address and the email server.

After blocking the connection, Savoy spoke with the FBI officer investigating the situation. Savoy learned that the FBI was getting a search warrant.

Later that night, Savoy logged on from home to check on the situation. Although the suspect computer was still blocked from accessing the network at the first IP address, it had logged on to the network with another IP address. This made Savoy worry even more that the email server was in immediate danger, because the intruder knew that he was being investigated and could interfere with the system to cover his tracks.

To make sure that the computer logged on at the new IP address was the same computer that had been logged onto the old address, he remotely logged onto the computer and looked into the temporary directory (without deleting, modifying, or destroying any files). Once he was sure it was the same computer, he logged off. At this point he was sure that the computer needed to be disconnected from the network immediately for the safety of the university network.

Savoy then went with university police officers to the dorm. He found the computer unattended and disconnected its network cord. After that, Heckenkamp was located, and he voluntarily provided his user name and password. Savoy used the username/password to run commands on the computer, and verified that it had been used to gain the unauthorized access.

Toledo Office:  
One SeaGate, 24th Floor  
P. O. Box 10032  
Toledo, Ohio 43699-0032  
Telephone: 419-241-6000  
Fax: 419-247-1777

Columbus Office:  
100 East Broad St.,  
Ste. 1300  
Columbus, Ohio 43215  
Telephone: 614-280-1770  
Fax: 614-280-1777

Findlay Office:  
725 South Main St.  
Findlay, Ohio 45840  
Telephone: 419-424-5847  
Fax: 419-424-9860

[www.eastmansmith.com](http://www.eastmansmith.com)

The Ninth Circuit Court found that the search of the computer was justified under the “special needs” exception to the warrant requirement, notwithstanding Heckenkamp’s reasonable expectation of privacy in his computer. The special needs exception applies where there are “special needs, *beyond the normal need for law enforcement*, [that] make the warrant and probable-cause requirement impracticable.”

The Ninth Circuit applied the special needs analysis as follows:

- (1) The special need beyond law enforcement was that of protecting the integrity of the university computer network, and Savoy was acting purely within his role as a systems administrator (and not as an agent of law enforcement) to meet that special need.
- (2) The need to protect the system was immediate. Although the FBI was going through the warrant process, Savoy as a network administrator thought that *immediate* action was required.
- (3) Requiring a warrant to investigate potential misuse of the university’s computer network would disrupt the operation of the university and the network.
- (4) Network administrators are different from law enforcement because they usually do not have the same kind of “adversarial relationship” with network users as police have with suspected criminals.

Finding a special need, the court then “assess[ed] the constitutionality of the search by balancing the need to search against the intrusiveness of the search.” The factors the court considered were (1) the privacy interests of Heckenkamp, (2) the government’s interests in performing the search, and (3) the scope of the privacy intrusion.

Applying the test, the Court found that the university’s “compelling interest” in protecting its network overrode Heckenkamp’s privacy interests, especially because the remote search of Heckenkamp’s computer was so limited. Because of the weight of the government interest and the relative unobtrusiveness of the search, the remote search was not unconstitutional. Therefore, the evidence obtained by the warrantless search was valid.

This case serves as a guide to university administrators concerning when and under what circumstances a remote search may be legal when faced with a disruption of the university’s information systems. Careful attention to the standards used in this case may protect a university from claims of an illegal search and seizure.

*Ms. Borman is a member of the Firm’s Public Law Practice Group and has significant experience in education law. For more information regarding this decision, please contact her by calling 419-241-6000.*

*Daniel Everson, a summer law clerk, assisted with this article. He will be graduating from Ohio State’s law school in May 2008.*

*Disclaimer: The articles in this newsletter have been prepared by Eastman & Smith Ltd. for informational purposes only and should not be considered legal advice. This information is not intended to create, and receipt of it does not constitute, an attorney/client relationship.*