SIDLEY AUSTIN LLP
SIDLEY

MAY 2007

INFORMATION LAW AND PRIVACY UPDATE

The Information Law and Privacy Practice of Sidley Austin LLP

We offer clients an inter-disciplinary, international group of lawyers focusing on the complex national and international issues of data protection and cyber law. The group includes regulatory compliance lawyers, litigators, financial institution practitioners, health care lawyers, EU specialists, IT licensing and marketing counsel, intellectual property, and white collar lawyers.

Sidley provides services in the following areas:

Privacy and Internet Litigation and Regulatory Advice
Data Breach, Incident Response, and Cybercrime Advice
Global Data Protection and Information Security
International Data Transfer Solutions
Outsourcing and Cross-Border Issues
Gramm-Leach-Bliley and Financial Privacy
HIPAA and Healthcare Privacy
Workplace Privacy and Employee Monitoring
Cyberlaw, E-Commerce, and Internet Issues
Unfair Competition and Consumer Protection
Trademark and Copyright Litigation and Counseling
Website Policies and Domain Name Protection
Records Retention and Electronic Discovery

For more information, please visit www.sidley.com/cyberlaw, or contact:

Alan Charles Raul
202.736.8477

To receive future copies of the Information Law and Privacy Update via email, please send your name, company or firm name and email address to rduncan@sidley.com

Ninth Circuit Rules on Privacy Rights in Personal Computers Connected to Networks

A recent Ninth Circuit decision interpreting the Fourth Amendment sheds light on the privacy rights of users of publicly-operated computer networks. In *U.S.* v. *Heckenkamp*, Nos. 05-10322, 05-10323 (9th Cir. Apr. 5, 2007), the court was called upon to determine whether a search of a student's hard drive by a university network administrator in the context of a computer hacking incident violated the Fourth Amendment. The court concluded that, while the student did have a reasonable expectation of privacy in the contents of his computer, the evidence acquired during the search was nonetheless admissible in a criminal prosecution under the "special needs" exception to the Fourth Amendment. The decision is noteworthy for affirming the principle that privacy rights are not forfeited simply through the act of connecting a computer to a network. At the same time, the court's opinion suggests that those rights in practice may be rather heavily constrained, as they must be balanced against the needs of network operators. Where a network operator has a legitimate need to search a user's computer, the Fourth Amendment may not be effective in shielding the user from later criminal prosecution.

The *Heckenkamp* case stemmed from the discovery of an intrusion into the network of California-based Qualcomm Corporation. A Qualcomm systems administrator identified a computer on the University of Wisconsin network as the source of the hacking activity, and contacted both the university and the FBI. The university's computer network investigator, Jeffrey Savoy, subsequently found that, in addition to accessing Qualcomm's network, an individual using a computer on the university network had also obtained unauthorized access to the university's own system. Further investigation revealed that the computer in question belonged to Jerome Heckenkamp, a University of Wisconsin computer science graduate student who had

Also inside:

been terminated from his position with the university's computer help department due to similar unauthorized conduct.

To assess the present risk to the university's system, Savoy performed a remote search of Heckenkamp's computer. Savoy also contacted the FBI investigator assigned to the Qualcomm matter to report his findings. The FBI investigator advised Savoy to refrain from further action until the FBI could obtain a search warrant. Out of concern that Heckenkamp's computer posed an imminent threat to the university's system, however, Savoy decided to take the machine off line immediately. With the help of university police officers, Savoy went to Heckenkamp's dorm room and disconnected the computer. Federal agents subsequently obtained a search warrant, which allowed them to seize Heckenkamp's computer and search his room. Heckenkamp was indicted on multiple offenses, and ultimately entered a conditional guilty plea to charges under the federal Computer Fraud and Abuse Act, 18 U.S.C. § 1030. Relying on the Fourth Amendment, Heckenkamp appealed the denials of his motions to suppress the evidence against him. The Ninth Circuit affirmed.

To resolve the question of whether Savoy's search was permissible under the Fourth Amendment, the court considered whether Heckenkamp had a reasonable expectation of privacy in his computer. The court concluded that Heckenkamp had both a subjective and "a legitimate, objectively reasonable expectation of privacy in his personal computer," and that his privacy expectations were not defeated by the act of connecting his computer to the university network. *Heckenkamp*, Nos. 05-10322, 05-10323, slip op. at 3887. The court made clear that "the mere act of accessing a network does not in itself extinguish privacy expectations, nor does the fact that others may have occasional access to the computer." *Id*. at 3888. While privacy expectations may be limited where network users are informed that their communications may be monitored, the university had no such announced policy. The fact that Heckenkamp's computer was protected by a password and kept in his dormitory room also weighed in favor of finding his expectation of privacy to be reasonable.

Despite this finding, however, the court ruled that Savoy's remote search of Heckenkamp's computer was justified under an exception to the Fourth Amendment. The special needs exception dispenses with the warrant requirement in circumstances where needs beyond those of ordinary law enforcement render the requirement impracticable. Since the court was satisfied that Savoy was acting purely as a system administrator and that his actions were unrelated to a need to obtain evidence for law enforcement purposes, the court held that the evidence was properly admitted under the special needs exception. In reaching this conclusion, the court underscored the interests of the university in protecting its network, and suggested that those interests may outweigh the privacy rights of network users. Despite Heckenkamp's legitimate expectation of privacy in his computer, "the university's interest in maintaining the security of its network provided a compelling government interest in determining the source" of the threat. *Id*. at 3891. Moreover, by connecting his computer to the network, Heckenkamp had in effect assented to a university policy allowing system administrators to respond to threats against network integrity.

The *Heckenkamp* case indicates that, while users of computer networks may retain a right of privacy in their personal computers under the Fourth Amendment, that right can be severely narrowed. In courts that follow *Heckenkamp*, the Fourth Amendment rights of individual users will be balanced against the interests of network operators. Particularly where there is a threat to network security, operators' interests will weigh heavily in that analysis. By relying on the special needs exception to uphold a criminal judgment in this case, the Ninth Circuit rendered those who misuse computer networks vulnerable to prosecution using evidence that, absent the interests of network administrators, the government lawfully could not have obtained.

A copy of the Ninth Circuit's decision is available at **http://www.ca9.uscourts.gov/ca9/newopinions.nsf/AE0DB21CF9CC371A882572B3007EB140/$file/0510322.pdf?openelement**

Appellate Court Rejects Fourth Amendment Privacy Claim of Employee Who Used His Own Personal Computer at Work

A federal appellate court has ruled that a city employee who brought his own computer to work and connected it to the city network had no reasonable expectation of privacy under the Fourth Amendment. In *U.S.* v. *Barrows*, No. 06-6274 (10th Cir. Apr. 3, 2007), a municipal treasurer sentenced to prison for child pornography offenses appealed the district court's denial of his motion to suppress evidence obtained from his personal computer, arguing that the government's search of his hard drive violated his Fourth Amendment rights. The Tenth Circuit held that mere ownership of one's computer is not sufficient to establish a reasonable expectation of privacy from government intrusion.

The *Barrows* case arose after a city police officer found pornographic images on the computer of treasurer Michael Barrows during an attempt to resolve a technical problem with a city-owned machine. Barrows, who shared both a workspace and a computer with a clerk in the city hall, had decided to bring his home computer to work so that the two would no longer need to use a single machine. Barrows connected his own computer to the city network and left it running constantly, taking no measures to prevent other employees from using his machine or accessing his files. When the clerk with whom Barrows shared a workspace began to experience access problems with the city-owned machine, she requested assistance from a police officer who possessed some technical expertise. Suspecting that the access problems were linked to Barrows' use of the network, the officer checked Barrows' computer and inadvertently discovered files containing child pornography. The officer subsequently seized Barrows' computer and obtained a warrant to search the entire hard drive. After entering into a conditional plea agreement in which he pled guilty to child pornography charges, Barrows relied on the Fourth Amendment to challenge the district court's refusal to suppress the evidence found on his hard drive.

Under the Fourth Amendment, a warrantless search may be deemed unreasonable if the individual possessed a legitimate expectation of privacy in the item searched. In this case, the Tenth Circuit determined that Barrows neither had a subjective nor a reasonable expectation of privacy in his computer. While the court emphasized that private ownership of the item in question is a factor that carries significant weight in the Fourth Amendment analysis, it is not dispositive. Barrows' actions, including his failure to protect his computer with a password or to take other measures to prevent third-party access, his decision to connect his computer to the city network for file-sharing purposes, and his use of the computer in an open space accessible to city employees and members of the public, all belied any expectation of privacy. In addition, according to the court, "the significance of personal ownership is particularly weakened when the item . . . is being used for business purposes." *Id.* at 5. Given the fact that Barrows had voluntarily brought his computer to a public workplace for work-related use, ownership alone could not demonstrate a legitimate privacy expectation.

The *Barrows* decision establishes that those who seek Fourth Amendment protections must have recourse to more than mere ownership to support their claims. When considered in light of a recent Ninth Circuit decision, Barrows also helps to define the contours of the rights of computer network users. In the Ninth Circuit case of *U.S.* v. *Heckenkamp*, Nos. 05-10322, 05-10323 (9th Cir. Apr. 5, 2007), which was decided two days after *Barrows*, the court set forth a presumption that merely connecting a computer to a network does not extinguish privacy rights, even where third parties occasionally have access to that computer. *Barrows* suggests that any such presumption may be overcome where an individual not only connects to a network, but also declines to take even basic precautions to protect a computer's contents.

A copy of the Tenth Circuit's decision is available at **http://www.ck10.uscourts.gov/opinions/06/06-6274.pdf**