“[Heckenkamp] may also impact the electronic privacy of persons whose computers are attached to certain networks, both in academia, and elsewhere, including persons who have committed no crimes.”

The Heckenkamp Ruling May Affect the Privacy of Innocent Citizens

David Carney

David Carney is an attorney who writes and publishes Tech Law Journal, an online publication offering news and analysis of legislation and litigation affecting computer and communications technology. In the following report he presents the background of United States v. Heckenkamp and explains the basis of the court of appeals’ decision. First, he notes, the court determined that Jerome Heckenkamp did have a reasonable expectation of privacy on his computer; however, it then ruled that it was legal for university officials to search its hard drive without a warrant because there is an exception to the rule that search warrants are necessary; they are not required when “special needs, beyond the normal need for law enforcement” make obtaining a warrant impractical. In this case, the university was motivated not by a desire to assist the FBI in its investigation of Jerome Heckenkamp’s alleged crimes, but by a concern that its computer network was threatened by hacking. The ruling, Carney argues, may affect many people, even those who have not committed crimes, because knowing that evidence obtained without a war-
rant need not always be suppressed will reduce the incentive for investigators to respect network users’ privacy.

April 6, 2007. The U.S. Court of Appeals (9thCir) issued its opinion in USA v. Heckenkamp, a Section 1030 case in which the issue is the admissibility of evidence acquired in a warrantless remote search of a student’s hard drive by a university network administrator who was acting in association with the FBI.

The Court of Appeals affirmed the District Court’s denial of Heckenkamp’s motion to suppress evidence under the special needs exception to the warrant requirement. The Court of Appeals held that federal prosecutors can use evidence collected in a warrantless computer search to prosecute a student for hacking computers outside of the university network, when the university acted out of an independent concern to protect its own computer systems.

Background. The Federal Bureau of Investigation (FBI) was investigating unauthorized access to the computer systems of Qualcomm. It determined that the intruder likely accessed Qualcomm’s computer systems from a computer on the University of Wisconsin (UW) network.

The FBI then sought and received assistance from the UW. A UW investigation of network information led it to focus on one individual, Jerome Heckenkamp, who was a graduate student in computer science, and the computer in his UW dormitory room. The UW investigation determined that a computer, or two computers, it was not sure, under investigation, may have been used to gain unauthorized access to both Qualcomm’s computer system and the UW e-mail system.

At this point, neither the FBI, nor UW police, had obtained a search warrant, or permission from Heckenkamp, to search his computer. Nevertheless, a UW network administrator used his computer to remotely search the hard drive of Heckenkamp’s computer.