Employment
LOS ANGELES DAILY JOURNAL • FRIDAY, APRIL 13, 2007 • PAGE 8

LIMITED Privacy: Searching Workplace Computers

By Nicole Kamm

Under the Fourth Amendment, private-sector employees enjoy protection for their work spaces, including contents of their work computers. Police must obtain a search warrant or consent to conduct a search. A recent 9th Circuit decision reaffirmed that employees can expect work space privacy, but the panel held that the employer can consent to a search of the employee's computer and the consent is valid under the Constitution, even if the employee does not consent. *U.S. v. Ziegler,* 2007 DJDAR 1345 (9th Cir. Jan. 30, 2007).

Fourth Amendment decisions distinguish between private-sector and government employees. The rules for warrantless searches in private workplaces resemble the rules for warrantless searches of a residence: Employees have privacy rights at work unless their work space is completely open to the public, and employers can consent to searches of spaces that are not open to the public.

The 1968 decision in *Mancusi v. DeForte,* 392 U.S. 364, involved a warrantless search by police of a union headquarters office that the defendant shared with other union officials. The defendant claimed the search violated his Fourth Amendment rights. The police responded that, because the office space was used jointly, the defendant's claimed expectation of privacy was unreasonable. The Supreme Court ruled for the defendant, holding that he "still could reasonably have expected that only [his co-workers] and their personal or business guests would enter the office, and that records would not be touched except with their permission or that of union higher-ups."

Because only a specific group of people had access to use of the office, the employee retained an expectation of privacy in his work space.

Government agents can overcome this expectation by obtaining consent of "a party who exercises common authority over the area searched." *U.S. v. Matlock,* 415 U.S. 164 (1974). In practice, this means the government can overcome the warrant requirement with the consent of the employer or supervisor. In some cases, a co-worker's consent may suffice.

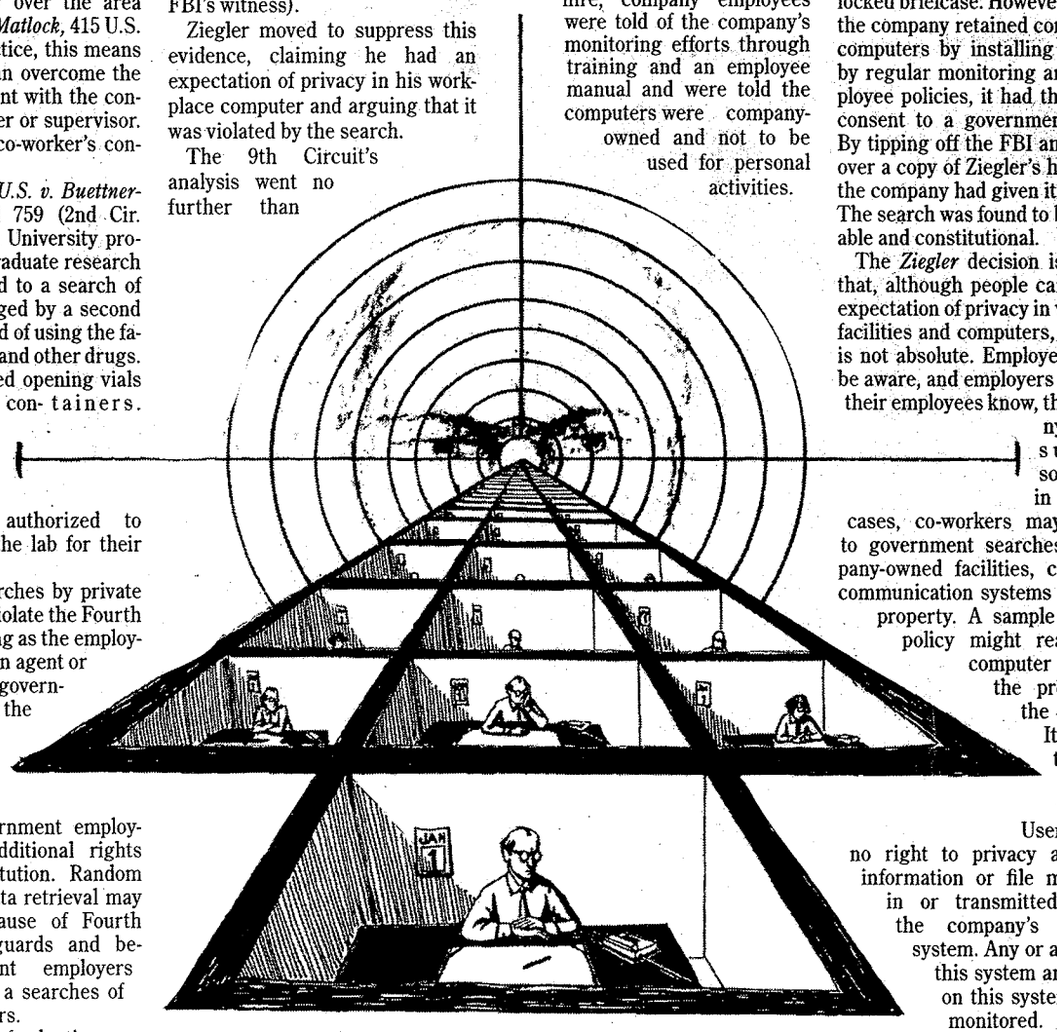
For example, in *U.S. v. Buettner-Janusch,* 646 F.2d 759 (2nd Cir. 1981), a New York University professor and undergraduate research assistant consented to a search of a laboratory managed by a second professor suspected of using the facility to make LSD and other drugs. The search involved opening vials and other closed containers. The 2nd Circuit approved the search because both consenting co-workers were authorized to make full use of the lab for their research.

Warrentless searches by private employers rarely violate the Fourth Amendment, as long as the employer does not act as an agent or instrument of the government at the time of the search. *Skinner v. Railway Labor Executives' Assoc.,* 489 U.S. 602 (1989). Government employees may have additional rights under the Constitution. Random monitoring and data retrieval may be improper because of Fourth Amendment safeguards and because government employers cannot consent to a searches of employee computers.

In *Ziegler,* the defendant's employer tipped the FBI after discovering that an employee accessed child pornography from a company computer. After the company determined that Ziegler was the person who downloaded pornography, the FBI wanted a copy of Ziegler's hard drive. The fact in dispute was whether the company copied the employee's workplace hard drive at the FBI's request (as testified to by the company witness) or previously obtained copies (according to the FBI's witness).

Ziegler moved to suppress this evidence, claiming he had an expectation of privacy in his workplace computer and arguing that it was violated by the search.

The 9th Circuit's analysis went no further than determining whether Ziegler had a reasonable expectation of privacy for the contents of his workplace computer. The court noted that the company required each employee to use an individual log-in and "had complete administrative access to anybody's machine." The company had installed a firewall to monitor Internet traffic, and monitoring was routine. On hire, company employees were told of the company's monitoring efforts through training and an employee manual and were told the computers were company-owned and not to be used for personal activities.



The court held that Ziegler "could not reasonably have expected that the computer was his personal property, free from any type of control by his employer."

On rehearing, the court agreed with Ziegler that an employee's computer should be protected from a government search under a reasonable expectation of privacy similar to that in a private office or locked briefcase. However, because the company retained control of its computers by installing firewalls, by regular monitoring and by employee policies, it had the right to consent to a government search. By tipping off the FBI and turning over a copy of Ziegler's hard drive, the company had given its consent. The search was found to be reasonable and constitutional.

The *Ziegler* decision is an alert that, although people can have an expectation of privacy in workplace facilities and computers, this right is not absolute. Employees should be aware, and employers should let their employees know, that company officials, supervisors and, in some cases, co-workers may consent to government searches of company-owned facilities, computers, communication systems and other property. A sample company policy might read, "This computer system is the property of the company. It is for authorized business use only. Users have no right to privacy as to any information or file maintained in or transmitted through the company's computer system. Any or all users of this system and all files on this system may be monitored. By using this system, the user consents to monitoring and disclosure at the company's discretion. The company reserves the right to disclose information concerning use of this computer system to law enforcement personnel, as well as officials of other government and private agencies. The company reserves the right to consent to government searches. Unauthorized or improper use of this system may result in disciplinary action, including termination as well as legal action. By using this system, you indicate your awareness of and consent to these terms and conditions of use."

Ziegler leaves open a question of whether employers who monitor employee Internet use take on a duty to investigate and report criminal activity. A New Jersey appellate court held recently that an employer having actual or implied knowledge that an employee used a workplace computer to access pornography, possibly child pornography, "has a duty to investigate and act to stop the unauthorized activity." *Doe v. XYC Corp.,* 887 A.2d 1156 (N.J. Super. Ct. App. Div. 2005). The court rejected the company's claim that respect for employee privacy justified its failure to act.

The court explained the employee had no expectation of privacy, because a written company policy both informed employees that their e-mail and Internet use would be monitored and prohibited improper computer use, and the employee's cubicle was open to the world at large.

Though not binding in California, *Doe* has significant implications. Courts that follow the decision may hold employers liable for failing to monitor Internet activities of their employees. Along with a workplace policy stating that employers can monitor computer use and that improper use is grounds for discipline, an employer who suspects an employee is using a computer for unlawful purposes should assess whether to investigate and take immediate action to stop the misconduct. If the misconduct involves criminal activity, employers also should consider whether to notify law enforcement.

Nicole Kamm is an associate at Lewitt, Hackman, Shapiro, Marshall & Harlan, in Encino.