THIRD DEGREE COMMUNICATIONS, INC.

TRAINING BULLETIN: LEGAL UPDATE

WORKPLACE SEARCHES

By Charles Gillingham

When I told my father I was going to become a lawyer, he cried. I thought they were tears of joy. I was mistaken. My father is a retired peace officer, as was my grandfather and uncle—my brother-in-law and cousin are working as officers. I am the black sheep of the family and my father's tears were clearly not tears of joy but rather intense concern. My father told me, "the worst thing a cop can do is spawn an attorney." Needless to say, my options as an attorney were and are, limited. I will get my revenge, however, as I have a case where he is a witness---cross examination may be a bit tough on the old man. Apropos of nothing, but a catchy intro to this month's topic---workplace searches.

REASONABLE EXPECTATION OF PRIVACY

Two federal appellate courts have recently addressed the privacy interest of employees in their workplace computers. Both cases involved searches for child pornography. The courts held that while employees may have an expectation of privacy in the workplace, that expectation is greatly reduced. The decisions also make it clear that employees may not have an expectation of privacy in private information on their work place computers. Moreover, officers may also be able to search the employee's personal computer without a warrant if it is used in the workplace. Remember what you learned in the academy, the Fourth Amendment has two prongs; the subjective expectation of privacy the suspect exhibits and whether that expectation is objectively reasonable.

U.S. v. ***Ziegler***

The 9th Circuit Court of Appeal, which is frequently viewed as the most defendant friendly Circuit in the country, addressed whether an employee has a reasonable expectation of privacy in his work computer in *U.S.* v. *Ziegler* (9th Cir. 2007) 474 F.3d 1184. Ziegler worked at a company that services Internet merchants. All employees at the company were on notice that there was a firewall program at the company and that their Internet activity could be monitored by the company. Of course, the employees were not told when, or if, such monitoring took place. Ziegler had password-protected his work computer and had a private-locked office.

The Internet Technology administrator noticed while monitoring Internet activity that Ziegler was accessing child porn websites on his workplace computer. The administrator

told the owner of the company of the discovery. The IT administrator put a monitor on the computer and copied Ziegler's cache files, obviously without telling Ziegler. Cache is a location on computers where website visits are logged and recently viewed images are stored. The owner and IT administrator checked the cache and saw that Ziegler was looking at websites containing child pornography. The cache also revealed that Ziegler was downloading child pornography on the work computer.

The owner of the company contacted the FBI. The FBI directed the IT administrator to copy the hard drive. The IT administrator got a key to Ziegler's private office and copied the hard drive without telling Ziegler. The company told the FBI that they would comply with any directives from the FBI and cooperate fully. The copy and hard drive were ultimately turned over to the FBI by the company without a warrant.

Motion to Suppress

Ziegler was charged with possessing child pornography and moved to suppress the evidence. Ziegler claimed his Fourth Amendment rights were violated when the FBI directed the IT admin to go into his office and copy the hard drive. Ziegler's motion to suppress was denied and Ziegler appealed to the 9th Circuit Court of Appeals.

The Court of Appeals determined that Ziegler had a reasonable expectation in his office and work computer. This ruling was consistent with a prior Supreme Court ruling that held that an employee has a reasonable expectation of privacy in the workplace.[1] (In this instance, Ziegler had a private office that was kept locked. The Court found this was enough to evidence a reasonable expectation of privacy. That there was a master key to the office did not diminish the expectation of privacy.)

Even though the court determined Ziegler had an expectation of privacy in the computer, the court ruled the search lawful. The court found the company possessed "common authority" over the office and workplace computer.[2] Consequently the company could give valid consent to law enforcement for the search of the office and computer without Ziegler's consent. Ziegler next contended that the workplace computer also contained personal information and therefore the company could not consent to the search. The court found that the consent was sufficient even if there was personal information on the computer because Ziegler had a reduced expectation of privacy in the contents of the computer.

U.S.* v. *Barrows [3]

Michael Barrows was also charged with possessing child pornography. Barrows worked for the city of Glencoe, Oklahoma as treasurer. Barrows shared a computer and workspace with another employee. Because the two employees could not use the computer at the same time, Barrows brought in his personal computer, connected it to the city network and used it to do city work. Barrows had no password protection and took no steps to defend the computer from other employees. In fact, Barrows would leave the computer running at all times-even in the evenings and when he was away from his desk.

Unfortunately for Barrows, the other employee's computer froze up and she wondered whether Barrows' computer was the cause of the difficulty. She asked a reserve police officer who had helped her with computer problems in the past to check it out. The officer, who happened to be a former computer salesman, tried to unfreeze the computer but failed. The officer saw Barrows' computer open on the next desk and wondered whether Barrows had the same program open. The officer opened the computer and saw a file sharing program running. The officer opened that program and saw sexually suggestive file names. When the officer opened the files he found child pornography. The officer seized the computer, called the Sheriff and a subsequent search warrant was executed to search the computer. Barrows plead guilty and challenged the search of his computer by the officer.

No Expectation of Privacy

In this instance, the 10th Circuit found that Barrows had no expectation of privacy in his personal computer. Barrows used his computer as a workplace machine, did not password protect the computer, and took no steps to keep others off of his computer but rather left it on for others to use. The court found that Barrows worked in a shared space cordoned off from the general public only by a counter. Other employees frequently entered the space to use the copier and fax machine and could easily see what was on the computer screen or mistake the computer for a work computer and simply use it. Because Barrows took no steps to safeguard his personal computers from others the court held he had no expectation of privacy in the computer.

When can an employer give consent?

The court in ***Ziegler***, gave guidance to help in determining when consent from an employer is valid. When faced with a workplace computer search or seizure officers need to determine the expectation of privacy of the employee and whether the company can consent to a search. The following questions can help make that determination.

- How much regular access to the workplace computer does the employer have?
- Is there a firewall or proxy Internet server that allows the company to track Internet access of the employees?
- Is there an employee handbook that spells out the IT policies in the company, including whether Internet access is monitored?
- Is there a banner on the computer when there is a log in explaining that the computer is for legitimate work purposes only?
- Does anyone else in the workplace have access to the computer?
- Are there any known safeguards that have been installed on the computer?

The answers to these questions will help in determining whether the employer can give consent to search computers and whether an employee has a legitimate expectation of privacy in the computer.

Chuck Gillingham is a veteran prosecutor and regular instructor for the California District Attorney's Association and the Federal Internet Crimes Against Children Task Force. Chuck also teaches the legal portion of Multidisciplinary Child Interviewing for Third Degree Communications, Inc.

---

[1] *Mancusi v. DeForte* (1968) 392 U.S. 364. An employee has standing to object to a search of a desk or cabinet in their private office.
[2] *U.S. v. Matlock* (1974) 415 U.S. 164. Third parties who possess common authority over premises or effects have the ability to give valid consent to a search.
[3] (10th Cir. 2007) 481 F.3d 1246.