www.HRhero.com

# FLORIDA
## EMPLOYMENT LAW LETTER

*Part of your Florida Employment Law Service*

G. Thomas Harper, Editor
www.HarperGerlach.com

*Vol. 19, No. 12*
*February 2008*

## What's Inside



## On HRhero.com

***FMLA Leave***
Combine the FMLA with state family and medical leave laws, and you've got the makings of an HR migraine. Go to www.HRhero.com/news to find the following pain relievers:

- Sample Policy — Family and Medical Leave
- Sample Form — Family or Medical Leave Request and Response
- HR Executive Special Report — FMLA Leave: A Walk Through the Legal Labyrinth
- Hot Topics: Family and Medical Leave



*EMPLOYEE PRIVACY*

# Court suppresses evidence from employer-owned computer

*Whose computer is it anyway? The answer to that question may not matter all that much if an employee has a reasonable expectation of privacy in his office computer. In the following case, the state of Florida is paying for a church's failure to implement a computer and Internet policy. Let's take a look at the lessons the case teaches us.*

## Behind closed doors

Eric Young was the pastor at Jacksonville's Ft. Caroline United Methodist Church, a local church under the authority of the Florida Conference of the United Methodist Church. All local United Methodist churches are governed in accordance with the Book of Discipline, and all ordained pastors agree to be subject to the rules in the book.

As pastor, Young was given a desktop computer and a private office at his small church. Although the computer was for him to use in his capacity as pastor, the church had no official policy on its use or others' access to it. The computer wasn't networked to other office computers, and it was kept in Young's private office.

The office had a special lock that had three keys. Young had two of them, and the office administrator kept the third in a locked credenza. No one was permitted to enter the office without the pastor's permission. In his absence, even the church administrator was allowed to enter only for limited business purposes, such as "delivering paperwork for him to sign." She wasn't permitted to log on to his computer when he wasn't physically present.

BellSouth, the church's Internet service provider, called and informed the office administrator that spam had been linked to the church's Internet protocol address. She then ran a "Spybot" program on the church's computers and found some "very questionable web site addresses." She contacted a member of the staff parish and an information technology person to have the computers examined. Child pornography was discovered on Young's computer.

The chair of staff-parish relations, Kenneth Moreland, called Richard Neal, the district superintendent of the United Methodist Conference, who instructed him to contact law enforcement officials and allow them to see the computer. Neal informed Young that he was not to return to the church. When the officers arrived, Moreland unlocked the pastor's office and signed a "consent to search" form for the office and computer. Neal and Moreland reasoned they had authority to provide consent under the Book of Discipline, by which Young had agreed to be bound when he was ordained.

The police search of the computer found child pornography. It is unlawful

Harper Gerlach PL — www.HarperGerlach.com — is a member of the *Employers Counsel Network*

EMPLOYERSCOUNSEL.NET

to view, access, or possess pornography involving children. Young was arrested at another location, where he was meeting with Neal. He agreed to talk with the officers, and after being given his *Miranda* warning, he was interviewed.

During the interview, the officer showed Young a printout from the computer listing bookmarked websites. When the officer asked, "You have no right to privacy on that computer?" Young responded, "I suppose not. . . . I hadn't really thought about it." When the officer stated, "It's like me, . . . my laptop in my truck, if my boss says hand it over, he can look at anything that's on there because it's not mine," Young replied, "I suppose technically you're right." He also made "incriminating" remarks about child pornography and consented to the police's search of a memory stick in his office.

Young was charged with possessing child pornography. The trial court granted his request to suppress the evidence obtained in the search and the statements he made during the police interview, making that evidence inadmissible at trial. The state appealed.

## Court's analysis

The court began its analysis by outlining the protections of the Fourth Amendment to the U.S. Constitution. The court noted that to be afforded constitutional protections, a person accused of a crime must demonstrate a "legitimate expectation of privacy" in the area searched or the item seized. The legitimate expectation of privacy consists of both subjective and objectively reasonable components, considered in context and within the "operational realities" of the accused's workplace, *not legal ownership or possession.*

The court looked at a number of factors to determine whether Young had an objectively reasonable expectation of privacy, including:

(1) whether the area or item was "reserved for [his] exclusive personal use";

(2) his relationship to the item;

(3) whether the item was in his immediate control when it was seized; and

(4) whether he took actions to maintain a sense of privacy in the item.

In examining the operational realities of the expectation of privacy involving a workplace computer, the court considered other factors, including:

(1) whether the office has a policy covering the employer's ability to inspect the computer;

(2) whether the computer is networked to other computers; and

(3) whether the employer regularly monitors computer use.

The court noted that if an employer has a clear policy allowing workplace computer monitoring, the employee has no legitimate expectation of privacy. In the absence of a policy, however, all the other factors must be considered.

If the person accused (in this case, an employee) demonstrates he had a legitimate expectation of privacy, the state must show the search and seizure were reasonable to be able to use the evidence procured in the search. To do that, the state must obtain either a valid warrant or valid consent. Valid consent can be obtained from someone who reasonably appears to have "common authority" over the premises.

The appeals court concluded that Young did have an expectation of privacy in his office computer because:

- he kept his office locked when he was away;
- others' use of his office was limited;
- there were special locks for his office;
- he was the sole regular user of his computer, and no one else stored information on it;
- there was no workplace policy about the employer's access to the computer; and
- the computer wasn't networked to other computers in the office.

The court then determined that Moreland's consent allowing the police officers to search the office and computer wasn't valid because the officers didn't ascertain whether he had "regular access to or control over the office and the computer." Basically, the court said, the officers should have asked more questions about Moreland's authority to search the office and the computer and followed up with someone with more authority before they began searching. The court suppressed all of the evidence obtained through the search as well as all of Young's statements in response to the officer's references to the computer printout. *State of Florida v. Young*, 2007 WL 4480737, Fla. 1st DCA, Dec. 26, 2007.

**No one was permitted to enter the office without the pastor's permission.**

## Moral of the story

The single most important lesson here is to be sure your company has a clear computer and Internet policy that includes a reference to your right to access and monitor company computers at all times. Network all of your computers if possible, and obtain software that monitors employees' use of illegal or inappropriate websites.

It's important to remember that this was a criminal case. The church terminated Young and removed him from his pastoral duties. The case wasn't about wrongful termination, and the church's use of the computer information in deciding to fire Young wasn't questioned. Nevertheless,

to protect your company — and society at large — you should have a straightforward computer and Internet policy that allows for prosecution in similar cases.

We may not have heard the last of this case. The state could decide to appeal the trial court's decision to the Florida Supreme Court. We'll keep you posted.

➥ *You can find sample language for creating a computer-use policy in the subscribers' area of www.HRhero.com, the website for Florida Employment Law Letter. Just log in, scroll down to HR Tools, and click on "Sample Policies & Procedures." If you need help, call customer service at (800) 274-6774.* ✤