



Off-Duty Discussion Groups Can Be Off-Limits to Employers

Insights

3.01.10

(Hospitality Update, No. 1, March 2010)

There is an inherent tension between an employee's right to privacy and an employer's right to monitor an employee's conduct – especially where the employer believes that the conduct may harm its business or otherwise subject it to liability. This tension has only grown with the rapid expansion of social media and the larger audience with which an employee may share his grievances.

Recently, a federal court in New Jersey addressed this tension. In that case two former restaurant employees were awarded compensatory and punitive damages after managers accessed a private online chat room and used information obtained from the forum to terminate the employees. The court upheld the jury's award and determined that there was enough evidence to find that the managers did not have authority to access the chat room and, therefore, violated federal and state law.

On a positive note, the court's decision provides employers with more guidance on how far they can go when monitoring their employees' off-duty conduct. *Pietrylo v. Hillstone Restaurant Group d/b/a Houston's*.

Talking About "Crap"

Brian Pietrylo was a server at Houston's Hackensack, New Jersey restaurant and, like millions of other people, maintained a MySpace page in his off-duty time. While his page was public, and therefore open for all to see, including his managers, Pietrylo also included a private chat group called the Spec-Tator. The Spec-Tator was a place for Houston's employees to "talk about all the crap/drama/and gossip occurring in [their] workplace, without having to worry about outside eyes prying in. . . ." According to the lawsuit, users of the Spec-Tator used the chat room to discuss wages, union activity, and political activity, among other things.

In order to join the Spec-Tator a user must have received an electronic invitation from Pietrylo which, if accepted, would allow the user to access the chat room using his or her personal email address and a password. Pietrylo invited several coworkers to participate in the Spec-Tator, but did not invite any members of management. He maintained the Spec-Tator in his off-duty time, and no employee accessed the forum using company computers.

One of the employees who was invited to join the Spec-Tator was Karen St. Jean, a greeter at the restaurant. St. Jean later provided her password to two managers who, in turn, provided it to one of the restaurant's regional managers. These managers then accessed the private chat room on multiple occasions with the greeter's password and were horrified at what they found. The site contained sexual remarks about customers and managers, references to violence and illegal drug use, and a copy of a new wine test that was to be given to employees. Houston's terminated Pietrylo and one other employee for posting offensive comments.

But How Did They Get There?

The two employees filed suit against Houston's alleging that the restaurant's managers violated the Stored Communications Act (SCA) and the New Jersey Wiretapping and Electronic Surveillance Act when they accessed the forum. The SCA is a federal statute that expands the protections of the previously enacted Electronic Communications Act, and creates privacy protections in electronic communications such as emails and discussions in chat rooms. The law makes it an offense to intentionally access stored communications without authorization, or to exceed the scope of one's authorization.

At trial, Houston's argued that the managers did not violate the SCA because they were given a password to access the chat room by a member of the group and, therefore, accessed the site with permission. Thus, Houston's liability ultimately turned on whether or not Ms. St. Jean provided the managers with her access information voluntarily and whether the managers exceeded the scope of their authorization.

In deciding that Houston's violated the SCA, the jury believed that St. Jean did not provide her password voluntarily. The court agreed and upheld the jury's verdict noting that the employee testified that she felt compelled to provide her manager with her password as she felt she would "have gotten in trouble" had she not done so. Furthermore, the court determined that there were reasonable grounds for the jury to determine that the managers intentionally accessed the Spec-Tator despite their knowledge of St. Jean's discomfort with their use of her password.

Lessons To Be Learned

Before you log on to check on your employee's off-duty conduct, keep the following questions in mind:

Is the information private or public? If employees place information on a public forum for all the world to see then it is unlikely that they will be able to later claim that they did not want you to see it. But as the *Pietrylo* case demonstrates, if the employee takes steps to limit access to such information, or to make such information private, gaining access by using someone else's credentials is not only a bad idea, it may be illegal. Furthermore, employees who are disciplined or discharged for their online conduct may have a claim for invasion of privacy if the employee can show that the information that you used was private.

Is the employee's off-duty conduct lawful? Even if you have authorization to access an employee's off-duty conduct, or the employee has posted it on a public page, you cannot necessarily discipline an employee for inappropriate, yet legal, conduct. Many states have laws that prohibit employers from disciplining an employee for engaging in lawful conduct while off-duty, or for engaging in political activity or speech. Your state may be one of them.

Do you have legitimate grounds for disciplining the employee? Most state laws prohibiting discipline for off-duty conduct provide exceptions that allow an employer to discipline or terminate an employee if the employee's off-duty conduct jeopardizes trade secrets, harms the employer's business, creates a material conflict of interest, or exposes the company to potential liability for harassment or discrimination.

Do you have a policy in place to deal with this? Employees need to know what you consider acceptable and unacceptable off-duty conduct. The best way to accomplish this is to implement a well-crafted policy that provides you with a legitimate basis for disciplining your employees and, at the same time, balances the employee's rights with your business needs.

Related People



George A. Reeves, III
Partner
803.255.0000
[Email](#)