

Password-protected comments off limits to boss, jury rules

June 25 2009, By Hugh R. Morley

In a time when chat rooms, social networking and online forums are commonplace, how far can a company go in monitoring them for negative comments from discontented employees before they are guilty of "cybersnooping"?

A case decided last week, involving two servers at the Houston's Restaurant in Hackensack, posed that question, and a federal jury in U.S. District Court in Newark found there were clearly limits.

The jury sided with servers Brian Pietrylo and Doreen Marino, concluding that Houston's managers violated state and federal electronic communications laws when they entered into a private MySpace page on which workers criticized the company.

On seeing the site, the restaurant managers fired the two servers for violating company rules that demand employees exhibit professionalism, teamwork and a positive mental attitude. The jury awarded them a total of \$17,000 in back pay and damages.

Zack Hummel, a New York attorney who specializes in labor law and Internet issues, said the case is one of a growing number that reflect the struggle to adapt workplace behavior to the online era.

"It's coming up more and more because we don't have chats around water coolers anymore," he said. "We e-mail. What we have done is, we are all communicating so much through these systems that we have

changed the way of society, and the law is scrambling to catch up."

At issue was a MySpace group created by Pietrylo and Marino -- at the time a couple living in Dumont -- called SpecTator.

They designed the group for fellow workers to privately discuss their grievances. Access was by invitation only through use of an e-mail address and password. And the postings included derogatory statements about customers and managers, graphic sexual language and "sarcastic comments" about Houston's "quality, service and standards" according to court documents filed by the restaurant.

The group was brought to the company's attention by a third worker, a greeter at the restaurant who was a member of the group, who showed the postings to a manager. She later gave her password and e-mail to another manager, at his request, and he showed the postings to company executives in San Francisco.

The couple's suit, filed against the restaurant's owner, Beverly Hills-based Hillstone Restaurant Group, claimed the company violated their right to free speech. The couple also accused the company of wrongful termination, invasion of privacy, and of violating the federal Stored Communications Act and the state Wire Tapping and Electronic Surveillance Control Act.

The jury found the company guilty only of violating the state and federal communications laws, and concluded that its actions had been malicious.

The federal law, enacted in 1986, was designed to reflect the shift toward electronic communications. Congress noted that while privacy was easy to maintain in a letter -- which could be sealed -- electronic communications had no such protection.

The law prohibits unlawful access to electronic messages and certain disclosures of electronic information. The servers argued that that the law creates civil liability if someone "intentionally accesses without authorization" an electronic communications facility, or "exceeds an authorization to access that facility."

Fred Pisani, a Tenafly, N.J.,-based attorney who represented Pietrylo and Marino, said the verdict showed that "the bottom line is, there are limits to what an employer can do."

"The message is there are things that are business and there are things that are personal," he said. "And some things are off limits."

But Glen Viers, a vice president Hillstone Restaurant Group, which owns the 45 Houston's restaurants, said he saw no broader significance in the case.

"Contrary to what the plaintiffs have been saying publicly, this was never a case about cybersnooping, the First Amendment or an invasion of privacy," he said. "At the end of the day, our company is better for not having these individuals employed by us."

Several attorneys said the key issue was really one of privacy, and whether the servers could reasonably expect the postings to remain off limits to their employer.

If the comments had been made in an open forum or using the company e-mail system, the company would have committed no violation by reviewing the contents, attorneys said. Moreover, they added, the company could legally respond as it did.

"Firing somebody because they bad-mouth the company would be legally acceptable," providing the worker did not have an employment contract,

said Gary Nissenbaum, a Union attorney who specializes in online issues.

But the company ran into trouble because the postings were sealed off by the use of a password, the attorneys said.

Although the greeter said she was not threatened in any way before giving up the password, the two servers argued in court that she did so only because she was asked for it by a superior, and felt under pressure.

The greeter also told the court that she didn't authorize the manager to share the passwords with [company](#) executives in San Francisco.

That enabled the servers to argue their privacy was violated, said Bernard W. Bell, a professor at Rutgers Law School, who teaches privacy law.

"The argument of coercion is the only aspect of this that gave the plaintiff success," he said. "If you are distributing these comments, or posting these [comments](#), on a site that is not password protected, there is very little argument that there is an invasion of privacy."

(c) 2009, North Jersey Media Group Inc.

Visit The Record Online at www.northjersey.com/

Distributed by McClatchy-Tribune Information Services.

Citation: Password-protected comments off limits to boss, jury rules (2009, June 25) retrieved 19 April 2024 from

<https://phys.org/news/2009-06-password-protected-comments-limits-boss-jury.html>

This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.