A Timely Analysis of Legal Developments

ASAP®

In This Issue:

July 2009

Ranting on the Internet about one's employer has become commonplace. When these rants appear on publicly accessible Internet pages, employers can access them, and, except in limited circumstances, can take adverse action based on the posting's contents. As a recent adverse jury verdict demonstrates, employers who access a restricted social networking site without proper authorization can face liability under federal and state laws intended to protect personal privacy. The risk will increase as employees use increasingly sophisticated privacy settings to limit access to their personal social networking pages.

Verdict Against Houston's Restaurant Demonstrates Risks of Accessing Employee's Restricted Social Networking Sites

By Philip L. Gordon

Ranting on the Internet about one's employer has become commonplace. When complaints are posted on a publicly accessible Internet page, employers have the same right as anyone in the general public to access the posting, and, except in limited circumstances, can take adverse action based on the posting's content.

As the Hillstone Restaurant Group, owner of the Houston's restaurant chain, recently learned after an adverse jury verdict, employers who access a restricted social networking site without proper authorization face potentially significant exposure under federal and state laws intended to protect personal privacy. With employees becoming increasingly sophisticated about using privacy settings to control access to their personal social networking pages, this risk will become only more significant over time.

Houston's Management Accesses A Restricted Rant Site and Fires the Site's Leaders

Houston's employee Brian Pietrylo established a group on MySpace, called "The Spec-Tator," with the stated purpose of "vent[ing] about any BS we deal with at work without any outside eyes spying in on us." In his opening post, Pietrylo explained that the group was "entirely private and [could] only be joined by invitation." He then urged group members to "let the s**t talking begin." Pietrylo's coworkers, including his co-plaintiff Doreen Marino, took Pietrylo at his word. Over time, Pietrylo, Marino, and their Houston's colleagues posted sexual remarks about Houston's management and customers, jokes about Houston's standards for customer service and quality, and references to violence and illegal drug use.

Karen St. Jean, a Houston's greeter and authorized rant group member, showed The Spec-Tator to a Houston's manager while dining at the manager's home. Subsequently, another Houston's manager asked St. Jean for her password, and St. Jean provided it. This manager and a regional supervisor of operations separately accessed the site. St. Jean testified at her deposition that she did not believe that she would be fired if she had refused the request for her password, but she did think she "would have gotten in

some sort of trouble." She also testified that she is "not good under pressure." She admitted thinking that other managers would access The Spec-Tator once she gave her password to one of the Houston's managers.

Pietrylo testified at his deposition that he viewed the site's content as "just joking." Houston's management, however, did not find the site's content to be funny. The regional supervisor who viewed The Spec-Tator testified that he considered its content to be adverse to Houston's four core values of professionalism, positive mental attitude, aim to please, and teamwork. The regional supervisor terminated Pietrylo and Marino.

Proceedings in the Trial Court

In their lawsuit against Houston's owner, Pietrylo and Marino alleged violations of the federal Stored Communications Act and invasion of privacy, among other claims. The federal statute prohibits unauthorized access to electronic communications, such as Internet postings, stored at an electronic communications provider, a term that includes Web hosts such as MySpace, Facebook, and LinkedIn. The Act specifically excludes from this prohibition access "authorized ... by a user of the service with respect to a communication intended for the user." Similarly, under New Jersey law, consent is a defense to a claim for invasion of privacy.

In the summary judgment proceedings, Houston's contended that it had no liability on either claim because St. Jean indisputably had authorized management's access to The Spec-Tator by disclosing her password in response to management's request. The district court rejected this contention, reasoning that St. Jean's deposition testimony created a factual dispute over whether she had freely given her consent. The court noted that "there is a dearth of authority regarding what it means for consent to be freely given." The court itself, however, did not establish a standard. The court merely concluded that St. Jean's deposition testimony regarding her concern over a potentially adverse employment action had she not disclosed her password created a factual dispute that required a jury trial to resolve the question whether St. Jean had freely given her consent.

The jury returned a verdict against Houston's on both the federal Stored Communications Act claim and the invasion of privacy claim. The jury awarded Marino nothing on her claim for emotional distress. (Pietrylo did not claim emotional distress.) However, the jury awarded each plaintiff the maximum backpay that could be awarded — $903 for Marino and $2,500 for Pietrylo, both of whom had quickly found new jobs after Houston's fired them. The jury also found that Houston's had acted maliciously, *i.e.*, had engaged in "intentional wrongdoing in the sense of an evil-minded act." That finding entitled plaintiffs to an award of punitive damages, which the parties had agreed before trial would equal four times any actual damages awarded. The actual damages awarded also triggered the Stored Communications Act's right of an aggrieved party to recover attorneys' fees, although the trial court has not awarded fees as of this writing.

The jury instructions and jury questionnaire shed some light on the jury's thinking. With respect to the federal Stored Communications Act claim, both the jury instructions and the jury questionnaire focused on the state of mind of the Houston's managers who accessed The Spec-Tator, rather than on St. Jean's state of mind, when she disclosed the password. Thus, the jury answered "Yes" to the question, "Did Houston's knowingly or intentionally or purposely access The Spec-Tator without authorization from Karen St. Jean?" On the invasion of privacy claim, the jury found that The Spec-Tator was "a place of solitude and seclusion designed to protect the Plaintiffs' private affairs and concerns," but that plaintiffs had no reasonable expectation of privacy with respect to their statements posted in The Spec-Tator. The most likely explanation for this apparently inconsistent result is that while access to the group's MySpace page was restricted, authorized group members could share their passwords with any person who was not a group member.

Lessons Learned

The jury's verdict demonstrates that employers should tread with caution when accessing an employee's restricted web page. The trial court's willingness to send the case to the jury even though no one in Houston's management had threatened St. Jean in any way and based solely on St. Jean's equivocal testimony concerning her state of mind suggests a relatively high standard for proving that an

ASAP® is published by Littler Mendelson in order to review the latest developments in employment law. ASAP® is designed to provide accurate and informative information and should not be considered legal advice.

employee's consent was freely given. At trial, a subtle shift occurred in the inquiry: the jury appeared to focus less on St. Jean's state of mind and more on the state of mind of the Houston's managers who accessed The Spec-Tator. Thus, the jury focused on whether St. Jean actually had informed the managers that she was freely sharing her password with them.

In light of the common assumption that subordinate employees may perceive some element of pressure when asked to respond to management's requests and in the absence of settled authority addressing when a user's consent is valid under the federal Stored Communications Act, employers should consider the following course of action when confronted with the need to access a restricted Web site. First, carefully evaluate the degree of necessity and forego access when the need does not justify the risk. Second, document the voluntary nature of the consent of the employee who provides access in a signed acknowledgement. The documentation could, for example, include the following statements: (a) the employee understands that she is providing a manager with her password; (b) the manager will use the password to access a group site in which other employees participate; and (c) the employee disclosing her password understands that she will not be subject to any discipline or adverse employment action if (i) she does not provide the password, or (ii) she revokes her consent or changes the password at some future date.

Finally, employers should recognize that while the total award in the Houston's case was relatively small, other awards could be much larger. The Plaintiffs in the Houston's case were terminated long before the significant downturn in the economy. In today's economy, backpay awards very well could be larger. In addition, the Stored Communications Act permits for an award of minimum statutory damages of $1,000 per violation. While there is not much case law on the issue, if that provision were read to permit an award of $1,000 per unauthorized access, the multiplier effect could result in substantial statutory damages. Notably, the larger the actual damages award, the greater the likelihood of a substantial punitive damages and fee award.

Philip L. Gordon is a Shareholder in Littler Mendelson's Denver office, and Chair of Littler Mendelson's Privacy & Data Protection Practice Group. He maintains a blog on employment related privacy issues at http://privacyblog.littler.com. If you would like further information, please contact your Littler attorney at 1.888.Littler, info@littler.com, or Mr. Gordon at pgordon@littler.com.

ASAP® is published by Littler Mendelson in order to review the latest developments in employment law. ASAP® is designed to provide accurate and informative information and should not be considered legal advice.