A Timely Analysis of Legal Developments

ASAP®

August 27, 2013

New Jersey Court's Decision Provides Roadmap For Access To Employees' Restricted Social Media Content

By Philip Gordon

With New Jersey poised to become the twelfth state to enact a social media password protection law and scant case law addressing the circumstances when and how an employer can lawfully access employees' restricted social media content, last week's decision by a federal district court in New Jersey provides much-needed guidance for employers on the question whether and when they can use an employee's restricted social media content, provided by a co-worker, to impose discipline. That question is critical for managers, in-house employment counsel and human resources professionals because disgusted co-workers frequently "rat out" employees who abuse or embarrass their employer on restricted social media pages or lie to their managers and then post evidence of their fibs on their restricted social media pages.

The New Jersey decision, *Ehling v. Monmouth-Ocean Hospital Service Corp.*, provides a classic example of this fact pattern. The plaintiff in the case was a paramedic at Monmouth-Ocean Hospital Service (MONOC) in New Jersey. After news media reported that a deranged 88-year old had killed a security guard at the Holocaust Museum in Washington, D.C., the plaintiff could not resist dashing off the following post:

> "An 88 yr old sociopath white supremacist in the Washington, D.C. Holocaust Museum this morning shot and killed an innocent guard (leaving children). Other guards opened fire. The 88 yr old was shot. He survived. *I blame the DC paramedics*. I want to say 2 things to the DC medics. 1. WHAT WERE YOU THINKING? and 2. This was your opportunity to really make a difference! WTF!!! And to the other guards . . . go to target practice."

(emphasis supplied). This post appeared on a Facebook news feed to each of plaintiff's 300 Facebook friends. One of those Facebook friends, also a paramedic at MONOC, was a real world friend of a MONOC manager. The Facebook friend forwarded the post quoted above and other posts from the plaintiff's Facebook wall to the manager/friend. The manager—in turn—shared plaintiff's posts with MONOC's Executive Director of Administration.

Concerned about the post, MONOC management disciplined the plaintiff. The hospital suspended her with pay and sent her a memo expressing concern that her comment demonstrated "deliberate disregard of patient safety." Plaintiff, who at that time was the President of New Jersey's Professional Emergency Medical Services Association (the Union), challenged this discipline before

the National Labor Relations Board (NLRB). The NLRB determined that the discipline did not violate the National Labor Relations Act (NLRA), likely because the plaintiff's post did not speak to the terms or conditions of her employment with MONOC or involve concerted activity among MONOC employees. The NLRB also determined that MONOC had not violated plaintiff's privacy.

Not to be deterred, plaintiff raised her allegation of a privacy violation in a subsequent lawsuit filed in federal district court in New Jersey after MONOC terminated her employment in February 2012. In her complaint, plaintiff alleged that MONOC had gained access to her "friends only" Facebook page because a "member of upper management summoned a MONOC employee, who was also one of [the plaintiff's] Facebook friends, into his office" and "coerced, strong-armed and/or threatened the employee into accessing his Facebook account on the work computer in his supervisor's presence." Based on this allegation, plaintiff asserted claims under the federal Stored Communications Act (SCA) and for common law invasion of privacy. The New Jersey court granted summary judgment in MONOC's favor on both claims and, in the process, provided important guidance for employers regarding access to employees' restricted social media content.

As background, the SCA protects from unauthorized access only "electronic communications" in "electronic storage" at an "electronic communication service," provided the communications are not "readily accessible to the general public." The court ruled that content on a restricted Facebook page satisfies each of these elements because (a) a Facebook post is an electronic communication; (b) Facebook is an electronic communication service; (c) Facebook archives user posts, thereby satisfying the requirement of "electronic storage"; and (d) a "friends only" Facebook page, by definition, is not publicly accessible. Although this decision is not binding precedent, the New Jersey court is the second federal district court to reach this conclusion. Consequently, unless and until contrary case law develops, employers should presume that the SCA protects all Facebook posts that are not publicly available. Employers also should note that whether social media posts are in "electronic storage" could vary depending on whether and how the host archives content. As a result, the SCA likely, but does not necessarily, protect all restricted social media content.

Even if the SCA protects social media content, access to that content by *any* authorized user is perfectly lawful. In the plaintiff's case, the co-worker and Facebook friend who disclosed the content to MONOC management was an authorized user because he was a legitimate Facebook user and the plaintiff had invited him to view her Facebook wall by sending him a friend request.

Plaintiff attempted to rebut MONOC's defense that her Facebook friend and co-worker was authorized to view her restricted content by alleging that MONOC coerced the co-worker into accessing plaintiff's Facebook wall. In advancing this argument, plaintiff relied implicitly on another New Jersey case, *Pietrylo v. Hillstone Restaurant Group, d/b/a Houston's Restaurants*. There, a jury found that Houston's violated the SCA because two managers used a hostess' log-in credentials to access a restricted MySpace page where co-workers were posting negative comments about management and customers. When ruling on post-trial motions, the trial court determined that sufficient evidence supported the jury's verdict because the hostess testified at trial that she thought "something bad might happen" to her if she did not disclose her log-in credentials to the managers. According to the trial court, that testimony demonstrated sufficient "coercion" for the jury to reject Houston's defense that the hostess had authorized the managers' access.

The MONOC case presents starkly different facts. Plaintiff's coworker and Facebook friend had independently and voluntarily disclosed plaintiff's Facebook posts to the MONOC manager. There was no evidence that the manager pressured or coerced the plaintiff's co-worker in any way. In addition, the manager did not ask the co-worker for his log-in credentials or "shoulder surf" his Facebook page. Accordingly, the court held that MONOC had proved its defense that the co-worker and Facebook friend was authorized to access plaintiff's restricted social media content.

While the SCA claim was the principal focus of the court's attention, the court also granted summary judgment for MONOC on the plaintiff's common law invasion of privacy claim. The court reasoned that an intrusion on a private sphere is a fundamental element of that claim. However, MONOC did not intrude on the plaintiff's Facebook page: MONOC did not access the page using her log-in credentials or the log-in credentials of one of plaintiff's Facebook friends, nor did MONOC direct plaintiff's co-worker to access the page. Rather, MONOC, the court found, was "the passive recipient of information that [it] did not seek out or ask for." Because there was no actionable intrusion, the court did not reach a particularly important and pressing issue, *i.e.*, whether plaintiff's Facebook page was private for purposes of a common law invasion of privacy claim given that plaintiff permitted 300 "friends" to access her page, and none of those "friends"— as was demonstrated by the co-worker—had any obligation to keep plaintiff's Facebook posts confidential.

Employers can take away the following important lessons from this case:

- Social media content that is publicly available is *not* subject to privacy protection under the federal Stored Communications Act, common law, or any other U.S. law or regulation.
- Employers do not violate an employee's privacy rights when a co-worker independently volunteers screen shots or other information concerning an employee's restricted social media content.
- If an employer makes a follow-up request to a volunteer to provide additional information from a restricted social media page, the employer should establish the voluntariness of the volunteer's subsequent actions, *i.e.*, inform the volunteer that no adverse employment action will be taken if the volunteer declines the request and no special benefit will be conferred if the volunteer provides additional information, and document this agreement in writing.
- Employers should note that even after obtaining a volunteer's free and voluntary consent to provide additional information, the volunteer should be instructed to provide only the minimum information relevant to the purposes of the investigation. There is, however, some degree of risk because the propriety of this type of access has not yet been addressed.
- Finally, employers should recognize that accessing restricted social media content directly—either by obtaining the employee's or a co-worker's log-in credentials or by "shoulder surfing" on the employee or a co-worker—raises significantly higher legal risks than receiving screen shots or oral reports from a co-worker about an employee's restricted social media content. Before pursuing the riskier method of investigation, an employer should determine whether the relevant jurisdiction has enacted a social media password protection law and, regardless, consult legal counsel on how to structure the investigation to reduce legal risk.

Philip Gordon, Chair of Littler Mendelson's Privacy and Data Protection Practice Group, is a Shareholder in the Denver office. If you would like further information, please contact your Littler attorney at 1.888.Littler or info@littler.com, or Mr. Gordon at pgordon@littler.com.