

New Jersey Federal Court Finds that SCA Exception Applies to Facebook Posting Shared by Co-Employee

4 min read

Aug 26, 2013

By: Ambrose V. McCall

In the case of *Ehling v. Monmouth-Ocean Hospital Service Corp.*, Civ. No. 2:11-cv-03305 (WJM) (D. N.J. Aug. 20, 2013), a federal district court in New Jersey granted an employer's motion for summary judgment, and thereby dismissed the employee's claims of violations of the federal Stored Communications Act, (SCA"), the Family Medical Leave Act, and other claims the employee made under New Jersey law alleging discrimination, invasion of privacy, and protected "whistle blowing" activity. We will focus today on the court's analysis and application of the SCA to the sharing of screen shots from the employee's Facebook postings. Before reaching that discussion, however, the court first had to review the relevant facts.

The employee was hired as a registered nurse and paramedic in 2004, and in 2008 became president of the Professional Emergency Medical Services Association - New Jersey union. The employee pointed to two sets of factual circumstances which she alleged inappropriately led to her discharge. The relevant incident for our discussion is related to her Facebook account.

During 2008 through 2009, the employee had a Facebook account with about 300 Facebook friends. Through privacy settings, she only permitted her Facebook friends to have entry to her Facebook wall. Those friends, however, included a co-worker paramedic, who without the employee's knowledge, was providing screen shots from her Facebook wall to a hospital manager. The manager was friends with the paramedic from a prior job, but was not in the same division as the sharing paramedic. Moreover, the manager never asked to receive the employee's Facebook postings, never had the password to any employee's Facebook account, and was frankly surprised that he was shown any postings. The posting at issue referred to a shooting incident that occurred at the Holocaust Museum in Washington, D.C., in which the employee was viewed as blaming the paramedics on the scene for helping the criminal shooter to survive. When the manager saw the postings, he provided them to the Executive Director of Administration. The employee was temporarily suspended with pay and sent a memo that noted concerns about her communications showing a "deliberate disregard for patient safety." The employee

filed a complaint with the NLRB, who ultimately found no privacy violation, and no violation of the National Labor Relations Act. The NLRB also noted that the hospital's management had not solicited the postings at issue.

The employee claimed that her employer violated the SCA, 18 U.S.C. 2701-11 by illegally gaining access to her Facebook wall post about the museum shooting. She stressed that she had activated privacy settings for her Facebook account which triggered coverage under the SCA. The employer denied that the SCA covered her Facebook account, but also contended that if the SCA covered such data, it qualified for one of the exceptions in the SCA. The court held that the SCA covered the employee's Facebook account, but found that the undisputed facts supported applying the authorized user exception so that the employer had no liability under the SCA.

When surveying the law on social media accounts, the court referenced the scarcity of authorities on the issue of whether the SCA covered social media sites. In reviewing the legislative history of the SCA, the court found that social networking sites were barely in existence when the Act was passed. For example, the SCA was enacted before the World Wide Web came into existence in 1990, and before the first web browser was launched in 1994. Still, the SCA was read as covering a broad range of electronic communications that would include Facebook postings.

The court further found that the employee's postings were archived and stored on backup servers, and therefore held in electronic storage as required by the SCA. Finally, and perhaps most important, the employee had taken steps to restrict public access to her Facebook postings, and therefore satisfied the need to show that her posts were configured to be private. ("The legislative history of the [...] suggests that Congress wanted to protect electronic communications that are configured to be private. In sum, the court interpreted the SCA to extend beyond emails or text messages so as to encompass social media site postings entered with sufficient privacy controls.

While the employee successfully hurdled the issue of SCA coverage, her claim stumbled because her Facebook wall postings were intended to be used by the sharing co-worker she authorized to access her Facebook account. The employee had authorized her co-worker to enter her Facebook account, and the co-worker voluntarily made screen shots of the employee's Facebook posts and delivered them to management without any supervisory requests for such data. The deposition testimony revealed that no one was summoned, ordered, or compensated to provide her postings to management. In sum, her co-worker was one of her Facebook friends, and therefore an authorized user who could access her posts. Finally, by authorizing her co-worker to see her Facebook posts, the employee had created a situation where her postings were "intended for that user" as the SCA requires. As a result, the authorized user exception of the SCA applied, meaning that the employer was not liable under the SCA and entitled to summary judgment in their favor.

What the *Ehling* case tells employers is to be aware that accessing social media site postings may violate the Stored Communications Act unless the "authorized user" exception or other protective provisions of the Act apply. Moreover, given the recent growth of state laws protecting employees from certain requests by employers for their social media site passwords or other data, employers should consider seeking counsel before reviewing any data from social media sites of applicants or employees.

Hinshaw & Culbertson LLP is a U.S.-based law firm with offices nationwide. The firm's national reputation spans the insurance industry, the financial services sector, professional services, and other highly regulated industries. Hinshaw provides holistic legal solutions—from litigation and dispute resolution, and business advisory and transactional services, to regulatory compliance—for clients of all sizes. Visit www.hinshawlaw.com for more information and follow @Hinshaw on LinkedIn and X.

Topics

Facebook, New Jersey, Privacy