



Facebook: The New Water Cooler – Not The New Vegas

Insights

11.05.13

(Healthcare Update, No. 4, November 2013)

As of June 2013, Facebook, the reigning social-media giant, had 1.15 billion monthly active users who spent an average of 8.3 hours a month on Facebook. During roughly the same period of time, Facebook users “liked” a Facebook posting 4.5 billion times a day and uploaded an average of 350 million pictures a day.

These statistics demonstrate that Facebook and other social-media platforms have become the new water cooler in the office. Employees debate season finales of television shows, opine about Miley Cyrus' dancing, and announce changes in their relationship status at least as often on Facebook as they do around the lunch table in the break room.

Communication through social-media sites is becoming an increasingly acceptable norm. More and more individuals regularly share details of their daily life and thoughts online. But the consequence for employers is that the same individuals who post about being annoyed by the long wait at the doctor's office are the employees who will post complaints about a workplace rule they find oppressive. The same individual who gripes on Facebook about the refereeing at a kids soccer game, is the same one who will vent about a new, stricter manager.

However, unlike Las Vegas, what happens on Facebook, does not always stay on Facebook. Content posted by employees online frequently spills over into the workplace. As a result, managers are being increasingly challenged to find a balance between employee privacy rights and enforcing workplace standards. A recent case underscores the importance of understanding privacy laws before taking disciplinary action.

Paramedic's Problematic Post

An employee of Monmouth-Ocean Hospital Service Corp. (MONOC) was a registered nurse and paramedic. During her employment with MONOC the employee became a familiar name to human resources and management by receiving six disciplinary notices, taking a half dozen FMLA leaves, and serving as the president of the union.

During her employment, she also maintained a Facebook page and became Facebook friends with several of her coworkers. She set her privacy settings on Facebook so that only Facebook friends

and not the general public could see content she posted. But unbeknownst to her, one of her coworkers and Facebook friends was taking screen shots of her Facebook page and providing them to a manager.

On June 8, 2009, she posted a statement on her Facebook page about a shooting that had taken place at the D.C. Holocaust museum. Her status update noted that the shooter had been shot by other guards, but survived. The employee wrote: "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!" The employee's Facebook friend took a screen shot of her page and provided them to a manager. The hospital suspended the employee based on concerns that her posts reflected a "deliberate disregard for patient safety."

The employee sued alleging that the hospital violated the federal Stored Communications Act by accessing her Facebook posts. The court ruled that while the federal law did apply to certain Facebook content, the hospital did not improperly access her post by viewing the screenshot taken by her coworker.

So, What's The Stored Communications Act?

The MONOC employee sued under the federal Stored Communications Act (SCA), which is a law passed in 1986 to protect the privacy rights of individuals in electronic stored communications. The problem with the law is that it was enacted before the introduction of the World Wide Web in 1990 and, therefore, its application to modern technology and communications has not been widely tested. As a result, courts and employers are both beginning to grapple with the law's impact on access to online content.

The law's primary premise is that it prohibits intentional access, without authorization, to non-public electronic communications. The court closely analyzed the law and concluded that Facebook posts are electronic communications within the meaning of the law. Additionally, the court concluded that because the employee had adjusted her privacy settings so that only friends could see her posts, her Facebook postings were non-public and, therefore, fell within the protections of the Stored Communications Act. Accordingly, her employer was prohibited from intentionally accessing her posts without authorization.

Authorized Vs. Unauthorized Access

After finding that the SCA protects the privacy of Facebook posts when individuals utilize privacy settings, the court next considered whether the access to the posting was unauthorized. The SCA contains an exception which permits access by individuals who were both authorized users of the communication service, and who were intended recipients of the communication.

The court found that the authorized-user exception applied to MONOC's viewing of the paramedic's postings. Its rationale provides insight for employers on how to handle reports of Facebook or online misconduct by employees. The basis for the court's finding was two-fold. First, her posting was accessed by someone that was a Facebook friend of hers and, as a result, had rights to view her

postings. Therefore, as her Facebook friend, her coworker was an intended recipient of her postings.

Second, the coworker was not coerced or pressured to turn over the postings. The court found that access to the Facebook posting was done by an authorized user because the employee's Facebook friend viewed and copied the postings voluntarily, and was not based on any coercion or request by his employer. The court inferred that had the employer or one of its managers pressured the coworker to provide copies of the paramedic's Facebook posts the access would have been unlawful.

The rationale behind the court's finding was that if the access to the Facebook postings had been made because of pressure from the employer, the employer would be the real entity accessing the postings and it was not an authorized recipient of the communication. But when a Facebook friend voluntarily turns over the information, the friend is an authorized user and intended recipient of the communication and there are no restraints on sharing the communication with others.

According to the court, the law presumes that a Facebook user assumes the risk that what happens on Facebook does not stay on Facebook, and that their Facebook friends can voluntarily share their postings with others.

In the case of MONOC's paramedic, the court ruled that the employer's actions were lawful because access was made by an authorized user, her Facebook friend, and turned over to the company voluntarily. Accordingly, it was permissible for the hospital to review the postings and take lawful disciplinary action against the paramedic.

Handling Facebook Follies

The MONOC case is a good reminder that it is important for employers to pause before taking any action based on content posted on a social-networking site. Ensure both that your access to the information is lawful, and that disciplinary action would be appropriate. If you become aware of a troubling post on a social-media site, the first question you should ask is whether the post is accessible to the general public. If it is generally accessible to the public, then you can lawfully view it.

But if the posting is not generally accessible to the public, then you should consider how you learned about the posting and whether any copies of the posting you have reviewed were provided voluntarily by someone who was authorized to see the posting. If access to the postings was made by someone who was not an authorized user, such as a coworker who has been pressured by a supervisor or manager to provide access to the posting, then you should not view the posting or take any action based on it.

Finally, before taking any disciplinary action, consider whether disciplinary action is consistent and lawful. The protections of Title VII and other laws against discrimination and retaliation apply to disciplinary action taken based on online misconduct. Therefore, any disciplinary action taken should be consistent with your policies and past practices.

should be consistent with your policies and past practices.

Additionally, the National Labor Relations Act protects nonsupervisory employees' rights to discuss the terms and conditions of their employment in a concerted manner. Accordingly, if an employee is posting comments or concerns about topics such as wages, hours, or treatment by a supervisor, those postings may be protected in some circumstances, and disciplinary action would be unlawful.

For more information contact the author at KLuchka@laborlawyers.com or 803.255.0000.