THOSE PRYING EYES:

POTENTIAL LIABILITY FOR EMPLOYERS ACCESSING EMPLOYEE SOCIAL MEDIA POSTS

BY LAURA THALACKER, ESQ.

Employee social media use creates many legal risks for employers, particularly when the employer accesses or monitors an employee's online postings. Consider the following hypothetical:

An employee, Sarah, calls into work on Thursday and says she is sick with the flu and will be out of work through the following Monday. On Friday, Sarah's co-worker, Elizabeth, approaches Sam, the human resources director, and tells him that Sarah is not out sick and, in fact, is attending a bachelorette party in San Diego.

How does Elizabeth know this? The two employees are "friends" on Facebook. Elizabeth has seen Sarah's Facebook posts, which include Sarah checking in at various bars in San Diego and posting pictures of the bachelorette party. The posts are visible only to Sarah's "friends," so Elizabeth offers to give Sam the user name and password for her own Facebook account so that Sam can view Sarah's posts for himself.

What should Sam do?

a. Thank Elizabeth for coming forward and accept Elizabeth's offer to allow him to log-in with her user name and password (the sooner the better, in case Elizabeth changes her mind or Sarah deletes her posts!)

b. Run in the opposite direction and pretend it never happened.

continued on page 16

THOSE PRYING EYES: POTENTIAL LIABILITY FOR EMPLOYERS ACCESSING EMPLOYEE SOCIAL MEDIA POSTS

continued fom page 15

C. Call competent legal counsel to weigh the pros and cons, and to determine a recommended approach.

Although Option A may seem reasonable and safe, given that Elizabeth offered to share this information, the scenario still raises thorny legal issues. For example, Sarah may claim, although she authorized Elizabeth to view the posts, she never authorized, or intended, for her employer to access the information; or, what if Elizabeth later claims she was coerced into providing Sam with the user name and password?

Option B is also appealing and, in fact, is what you may be inclined to jokingly recommend to clients (because of the legal landmines this scenario presents). However, given the possibility of claims by either Sarah or Elizabeth, the best answer for the employer is C: seek competent legal counsel and obtain advice before opting to use Elizabeth's log-in credentials.

Versions of this hypothetical have been playing out in courts nationwide and are now further impacted by employee password protection laws, adopted in numerous states, including Nevada. The facts inevitably vary; instead of an employee, like Elizabeth, offering up a Facebook username and password, the employee may be offering log-in credentials for a chat room. Alternatively, sometimes the well-intentioned employee simply prints off the posts and provides copies to the employer. Other times, the employer inadvertently gains access to an employee's personal social media or email account when the employee forgets to log out of an employer-owned computer or mobile device.

These cases all raise a common question: To what extent can an employer lawfully view online employee information that the employee has designated as private, or to which the employee has otherwise restricted access?

This article discusses this question in light of two laws, the federal Stored Communications Act and NRS § 613.135.[1]

The Stored Communications Act, 18 USC §§ 2701-2711 (SCA)

Employees in situations similar to Sarah's have sued employers under the SCA. In very broad terms, this law (which was originally aimed at computer hacking and passed in 1986, long before the advent of social media) prohibits unauthorized, intentional access to private electronic communications, transmitted via an electronic communication service and stored electronically.[2] Courts addressing the question have ruled that the SCA covers non-public (i.e., private) social media posts (such as, in the hypothetical, Sarah's bachelorette party postings, visible only to her "friends" on Facebook).[3] However, the analysis does not end there. Although private social media posts have been deemed protected by the SCA, a court recently ruled that the authorized user exception to the SCA applied and the employer had not violated the law by reviewing copies of the plaintiff's Facebook posts, voluntarily provided to the employer by a co-worker who was the plaintiff's Facebook "friend."[4]

Other illustrative cases under the SCA include:

- *Konop v. Hawaiian Airlines, Inc.*, 302 F.3d 868, 879-80 (9th Cir. 2002) (holding, *inter alia*, that a private bulletin board on an employee's secure website was covered by the SCA and reversing summary judgment for the employer, where two of plaintiff's co-workers, who themselves were not active users of the website, voluntarily provided a management employee with their user names for gaining access to the website).

- *Pietrylo v. Hillsdale Restaurant Group*, No. 06-5754 (D. N.J. Sept. 25, 2009) (refusing to set aside a jury verdict in favor of a plaintiff-employee under the SCA where company managers accessed an invitation-only MySpace group by using another employee's log-in credentials; the employee who provided the credentials testified she felt pressured and was afraid she would get in trouble if she did not provide the log-in information to her managers).

- *Maremont v. Susan Fredman Design Group, Ltd.*, No. 10-c-7811 (N.D. Ill., March 3, 2014) (allowing an employee to proceed to trial on a claim that her employer violated the SCA by accessing her Twitter and Facebook accounts while she was recovering from a work-related injury, where there was a factual question regarding whether the employee had granted the employer permission to access the accounts).

Nevada's Social Media Password Protection Law, NRS 613.135

Elizabeth offering her log-in credentials to Sam also implicates Nevada's social media password protection law (NRS § 613.135), which took effect on October 1, 2013. This law precludes an employer from, directly or indirectly, requiring, requesting, suggesting or causing an employee or prospective employee to "disclose the user name, password, or other account information that provides access to his or her personal social media account."[5] A social media account is broadly defined as "any electronic service or account or electronic content, including, without limitation, videos, photographs, blogs, video blogs, podcasts, instant and text messages, electronic mail programs or services, online services or Internet website profiles."[6] The law further prohibits employers from taking any adverse employment action against employees or prospective employees for failing, refusing or declining to provide such information.[7]

Because Sam did not ask for, or otherwise compel, Elizabeth to provide her social media log-in credentials, NRS § 613.135 would appear not to have been violated. However, thoroughly documenting the circumstances to demonstrate that Elizabeth initiated the conversation and freely offered to share the information with Sam would be critical for preventing employer liability.

Advice for Sam, the Human Resources Director

What would you tell Sam if he came to you for legal advice? It is certainly not in the employer's best interests to look the other way when an employee misses work by falsely claiming to be sick. On the other hand, the employer must avoid engaging in any illegal conduct in its investigation.

Nevada courts have not ruled on the applicability of the SCA to social media posts, and case law in other jurisdictions is insufficiently developed to give Sam the green light to use Elizabeth's log-in credentials, even if voluntarily provided. Likewise, no Nevada courts have applied newly adopted NRS § 613.135. Under these circumstances, it would be risky for Sam to use Elizabeth's log-in credentials, and the employer should consider alternative options, such as the following:

1. Searching online to see if there is publicly available information about the bachelorette party (thus obviating any need to use Elizabeth's log-in credentials). Sarah may have shared photos on other social media sites (Instagram, Pinterest, etc.), that are visible to the general public;
2. Declining to use Elizabeth's log-in credentials but having Sam tell Elizabeth he would be interested in viewing a print-out of the posts if she wants to share them (perhaps resulting in Elizabeth voluntarily copying the posts and giving them to Sam);
3. Telling Sarah when she returns to work on Monday that Sam received a report that she lied about being sick and that she was actually in San Diego. This may prompt Sarah to admit her misconduct, thereby resolving the matter without the necessity of the employer viewing the social media posts.

As the hypothetical demonstrates, employers walk a fine line when balancing the right to manage their workforce with competing employee privacy interests. Courts and legislatures will no doubt struggle to keep up with changes in technology and the social media revolution. Whenever tempted to monitor or access employee social media posts, prudent employers are well-advised to step back, think twice and seek competent legal counsel. ■

---

1. Other claims, for example, privacy torts, potentially apply to this type of case, but are beyond the scope of this article.
2. 18 USC § 2701(a)(1).
3. *See Crispin v. Christian Audigier, Inc.*, 717 F. Supp.2d 965 (C.D. Cal. 2010); *Ehling v. Monmouth Ocean Hosp. Serv. Corp.*, No. 2:11-cv-03305 (D. N.J. Aug. 20, 2013).
4. *Ehling,* No. 2:11-cv-03305; *see also* 18 USC § 2701(c)(2) (excepting from liability "conduct authorized ... by a user of that service with respect to a communication of or intended for that user").
5. Among other exceptions, the law allows employers to obtain user names, passwords and account information (other than for a personal social media account) to access the employer's "own internal computer or information system." NRS § 613.135(2).
6. NRS § 613.135(4).
7. NRS § 613.135(1)(b).

LAURA THALACKER is a management-side employment lawyer with Hartwell Thalacker, Ltd. and a certified Senior Professional in Human Resources. Thalacker tweets on legal issues related to employee social media use @Fired4Facebook.