The Recorder
November 4, 2013

Employment Litigation in the Age of Social Media

Attorneys must balance the obligation to preserve evidence with restrictions on employers' access to employee accounts, explain Sheppard Mullin attorneys.

Paul Cowie and Marlene Nicolas

Like everything else, employment litigation has gone social, turning "likes" and off-the-cuff comments into high-stake courtroom drama. Social networking platforms like Facebook and Twitter have increasingly become litigation resources, providing a wealth of statements and images used to contradict the claims or defenses of the opposing party. While employers and their counsel must be aware of what is discoverable, as well as the technology and methods used to obtain social media evidence, they must also be careful to understand and adhere to potentially conflicting legal obligations. That is, they must balance the duty to preserve evidence against the prohibitions limiting an employer's ability to access or monitor an employee's social media activity. As some have discovered, failure to adhere to these laws can have severe consequences.

The Duty to Preserve Evidence

Common to all litigation, including employment litigation, is the litigants' duty to preserve potentially-relevant evidence. The duty serves the basic purpose of allowing litigants' access to the evidence needed to prove their case, or in a more idealistic sense, access to justice. As such, the consequences of failing to preserve potentially-relevant social media information can result in punitive sanctions against a party and their counsel. Indeed, cases have effectively been won and lost because a party has failed to preserve documents — known as spoliation.

For example, on July 17 Virginia lawyer Mathew Murray received a five-year suspension for telling his client, a plaintiff suing over the death of his wife, to clean up his Facebook account. In *Lester v. Allied Concrete Co.*, (2011), counsel for the defendants requested production of all pages from plaintiff's Facebook page as of the date the response was signed. Attached to the request was a picture of plaintiff partying with several young adults and clutching a beer can while wearing a T-shirt emblazoned "I [heart] hot moms." After receiving defendants' request, on March 26, 2009, Murray's office sent plaintiff an email wherein plaintiff was told to "clean up" his Facebook page because "we do *not* want blowups of other pics at trial; so please, please clean up your facebook and myspace." Plaintiff deleted 16 photos from his account, including the "I [heart] hot moms" photo. Plaintiff also deactivated his Facebook account the day before the response was due.

On the day the response was due, Murray served the following response: "I do not have a Facebook page on the date this is signed, April 15, 2009." When the defense filed a motion to compel, the plaintiff reactivated his account, denying at deposition that he had previously deactivated it. Defendants also filed a motion for sanctions, which was granted. The court ordered a combined $722,000 in sanctions against the plaintiff ($180,000) and Murray

($542,000). The sanctions were based on the expenses and fees incurred by defendants as a direct result of Murray's violations, including drafting the motion to compel, preparing for the hearing, and costs of retaining and deposing expert witnesses necessary to prove spoliation. The court also referred Murray's violations to the Virginia State Bar, which resulted in a five-year suspension.

In *Gatto v. United Air Lines, Inc.*, (2013), the plaintiff claimed he was injured on the job. In the course of a discovery dispute over the defendant's access to plaintiff's social media account, plaintiff was ordered to execute an authorization for the release of documents and information from Facebook. Plaintiff also agreed to temporarily change his account password to effectuate the same. Using the new password, defendants accessed the account to "confirm the password was changed," and printed portions of Plaintiff's Facebook page that contained comments and photographs that contradicted the plaintiff's claims and deposition testimony.

Soon thereafter, the plaintiff received notice that his Facebook account had been accessed from an unknown computer. Not knowing that defense counsel had accessed the account, the plaintiff deactivated his account, which resulted in all of the information and documents being deleted by Facebook's automatic 14-day deletion practice. Defendant requested that the court penalize plaintiff for spoliation. The court determined that an adverse jury instruction was appropriate, finding that "it is beyond dispute that plaintiff had a duty to preserve his Facebook account at the time it was deactivated and deleted." Significantly, the court gave short shrift to the plaintiff's claim that the act was unintentional stating, "[e]ven if plaintiff did not intend to permanently deprive the defendants of the information associated with his Facebook account, there is no dispute that plaintiff intentionally deactivated the account. In doing so, and then failing to reactivate the account within the necessary time period, plaintiff effectively caused the account to be permanently deleted."

As these cases demonstrate, employers and their counsel must take affirmative action to ensure that social media content is preserved by all parties early in litigation. Prior to discovery, counsel should serve a litigation hold letter on the employee's counsel and make clear that the employee and counsel have a duty to preserve potentially-relevant social media information, in its current state, and must not alter or delete any information or deactivate any such accounts. The letter should also make clear that the employee and counsel have an affirmative duty to familiarize themselves with any relevant social media site's terms of use and ensure that the service provider does not destroy the information. Failure to follow this instruction can be used to refute any claim that spoliation was unintentional.

It can also be useful to provide opposing counsel with specific instructions on how to save and or download information from the various sites. This is where understanding the technology is crucial.

For example, Facebook allows users to download every non-deleted item a user has ever posted to Facebook publicly or privately. Obtaining this information is relatively simple: a user need only click on "Account Settings," scroll down and click "Download a copy of your Facebook data," and then follow a few simple instructions. The user receives an email that includes a .zip file containing the following: profile/bio, status updates, wall posts, comments, images, videos, lists of current and former "friends," as well as the user's private messages both sent and received. Similar applications such as "TweetBackup," "Tweetake," and "BackupMyTweets"

allow Twitter users to back up followers, friends, favorites, and their own tweets and direct messages.

Prohibitions Limiting Access to Social Media Activity

Corporate social media accounts, as well as the personal accounts of employees may also contain discoverable information that needs to be properly preserved. Therefore, whenever litigation is reasonably anticipated, employers should issue a comprehensive "litigation hold" letter to all relevant personnel. The letter should include an instruction that employees must immediately identify and preserve any potentially-relevant documents and information, including social media information. That said, employers and their counsel must properly balance the duty to preserve evidence against the prohibitions limiting an employer's ability to access or monitor an employee's social media activity. This dichotomy can make it difficult for employers to ensure compliance with their preservation obligations.

An employer's ability to access, monitor, or act on social media posts by its employees is subject to state and federal limitations. These laws limit an employer's ability to request access to, or require an employee to grant access to, the employee's personal social media account(s). This includes asking an employee to "friend" counsel or company personnel in order to view the employee's account. To date, 12 states (Arkansas, California, Colorado, Illinois, Maryland, Michigan, Nevada, New Jersey, New Mexico, Oregon, Utah and Washington) have passed laws prohibiting employers from requiring employees or job applicants to provide login information or allow employer access to their accounts on social media sites.

Further, the federal Stored Communication Act prohibits certain access to electronic communications that are deemed to be in "storage" and that are "not public." Recently a New Jersey district court held that an employee's non-public Facebook wall posts were protected by the SCA. In *Ehling v. Monmouth-Ocean Hospital Service Corp.* (2013), the plaintiff employee alleged that her Facebook wall posts were covered by the SCA because she selected privacy settings limiting access to her Facebook friends, and therefore, her employer violated the SCA by improperly accessing her Facebook posts. The court agreed the employee's posts were covered by the SCA because she used privacy settings that limited access. However, the court found that the SCA's "authorized user" exception applied to defeat that protection because the employer learned of the post from one of the employee's co-workers, who was her Facebook "friend." Because the co-worker was an "authorized user" who voluntarily provided the post to the employer, the court rejected the employee's SCA claim and granted summary judgment. It is unclear if the result would have been different had the employer asked the co-worker to provide it with a copy of the employee's Facebook post.

While employers in several states, including California, cannot ask an employee to provide them access to a private social media account, they can view public social media accounts, steering clear of both state and federal law limiting such access. Also, although *Ehling* does not address the SCA's protection of posts that were public at the time they were made (i.e., not subject to Facebook's privacy settings), it is not likely that such posts would be protected by the SCA because they were public at the time they were made. This latter point is significant in the employment context where it is common for employees to change their privacy settings just prior to or during litigation.

As social media develops so too do the conflicting laws protecting employee's privacy and the employer's right to access such information. In light of these case law developments, employers should review their litigation hold practices to ensure that social media is properly secured both internally and by opposing parties.

Paul Cowie is a partner in labor and employment in Sheppard Mullin's Palo Alto office. Marlene Nicolas is a senior associate in labor and employment in Sheppard Mullin's Los Angeles office. Paul can be contacted at 650-815-2648 or pcowie@sheppardmullin.com. Marlene can be contacted at 213-617-4191 or mnicolas@sheppardmullin.com.