Social Media At Work: A Growing Danger

By Eli M. Kantor and Zachary M. Cantor

There is a growing danger in the workplace for employers and employees alike: Facebook and its brethren. Technology is constantly evolving, far more rapidly than privacy jurisprudence, which comparatively stumbles along like a decrepit wagon. Social media platforms, and the devices used to access them, pose significant problems for employee privacy and employer interests. That is why every employer must have technology policies that strike a balance between respecting employees' privacy and maintaining company integrity.

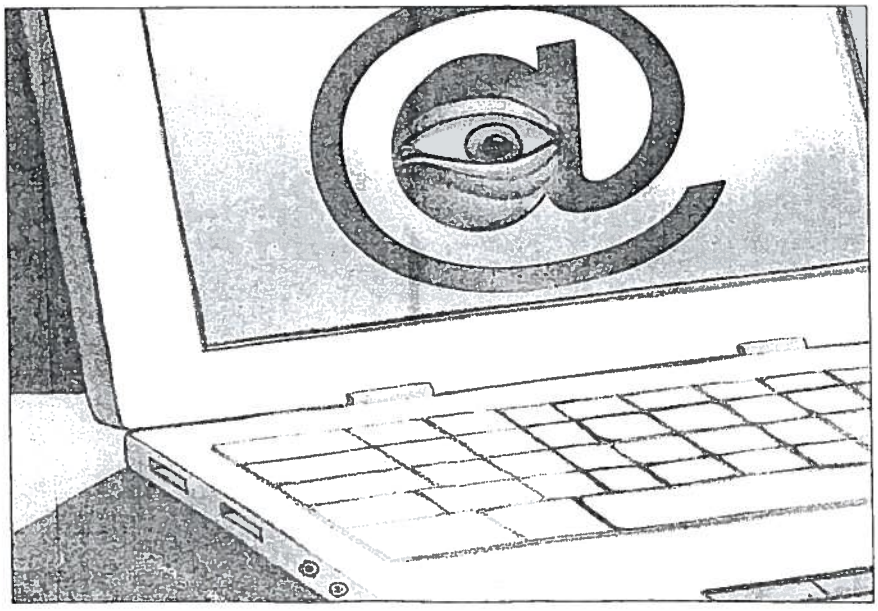
Many employers consider social media a remote cultural trend that has little significance for business. Likewise, the general public tends to think that if it's on the computer, it is private. Nothing could be further from the truth. Indeed, modern social media gives new meaning to the phrase: Life and death is in the power of the tongue.

Consider the Domino's Pizza debacle last April. Two employees posted a video on YouTube depicting their brazen health code violations, such as passing gas on sandwiches and stuffing cheese into their noses, while preparing food. Worse than the video, which garnered millions of viewers, were the comments that traumatized customers posted on Twitter. Because Dominos had no Twitter account to combat the blitz, it was defenseless. Needless to say Dominos opened a Twitter account the next day to address customer concerns.

For this reason, we were given the teeth and the lips as our two guards from slights of the tongue. These protectors must be strong, yet adaptable. Employers need to implement shielding policies, but also promote their business. Bear in mind the purpose of social media is an outreach tool. It enables every employee to be a spokesperson for the company — whether the company likes it or not. Hence, while employers must curb carelessness, it is important not to stifle creativity.

A sound policy should make clear to employees that only "public" information, like press releases and marketing materials, may be shared on social media sites — that is, if the company wishes to offer any leeway at all to its employees. And firmly insist that only "public" information may be used on social media sites. Moreover, since social media is constantly evolving, the policy must be broad enough to anticipate future, more dynamic media platforms. For example, Apple recently released the iPhone 4, enabling video-phone calls, which, in Apple's words, "Changes everything. Again." If you thought Twitter's instant text feed was too tempting for American impulsivity, wait until you can upload live video from your mobile device. A robust company policy will restrict the *content* of what employees can broadcast, rather than the *platforms* they can use. The result limits what employees can say, but not how they can say it — as not to hamper ingenuity. It will also put employees on notice that the company may review their messages.

However, employees may contend that they have a right of privacy, at least as to their own social media.



This is not the case since last year's California Court of Appeal decision in *Moreno v. Hanford Sentinel Inc.* (2009) 172 Cal.App.4th 1125. The court stated that by posting on Myspace.com, the material on Moreno's profile was provided "to the public at large. Her potential audience was vast." The court reasoned that Myspace.com is "a hugely popular internet site," and that "no reasonable person would have had an expectation of privacy" regarding postings on the site. Despite whatever settings an employee may have in place, social-networking sites are not private because profiles are available for so many to see. That is why the company policy should extend to both personal and company social networking sites.

Still, employers must go a step further. By setting clear parameters of what is permitted on social media as to the workplace, you put the employee on notice. But employees must do more than simply read the policy. Employees should be required to sign off on the fact that they have read and understood the policy. That way, should a lawsuit arise regarding wrongful termination for example, an employer can point to a signature that attests to the employee's knowledge of company policy. To that end, the human resources department should also thoroughly explain the policy, and field any queries an employee might have.

In addition to evolving social media platforms, technological advancements in workplace equipment have called privacy rights even further into question. Although the recent U.S. Supreme Court decision in *City of Ontario v. Quon*, 2010 DJDAR 9072, addressed government employers, the decision has far-reaching practical implications for private sector employers.

In Quon, the police department reviewed officer Jeff Quon's text messages — explicit messages he sent over a city-issued pager during work hours. Quon argued that the city's actions violated his Fourth Amendment right to be free from "unreasonable searches." The Court did not address whether Quon had an expectation of privacy, but it assumed that he did. And it held that the city's search was reasonable. The Court said the limits were minimal, so long as the employer's search of an employee's desk or text messages was for a "work-related purpose." The mind races to conjure potential work-related purposes.

After questioning the extent of employee privacy rights, the *Quon* Court pronounced: "[E]mployer policies concerning communications will of course shape the reasonable expectations of their employees, especially to the extent that such policies are clearly communicated." In *Quon*, the usage policy stated that messages may be audited, but the established practice was not to audit the messages so long as employees paid overage charges. Quon unsuccessfully argued that his superior's oral assurances overrode the contradictory written policy.

Quon may have broad implications. As an initial matter, *Quon* may affect the private sector. Although the Fourth Amendment only restricts government action, courts' treatment of Fourth Amendment issues may well influence employers' dealings with workers in private sector offices and factories. Further, in California, the state constitution expressly protects citizens from an invasion of privacy by *anyone* — not just the government. As Article I, Section 1 of the California Constitution states, "All people are by nature free and independent and have inalienable rights. Among these are enjoying and defending life and liberty, acquiring, possessing, and protecting property, and pursuing and obtaining safety, happiness, and *privacy*." While an invasive search claim under the U.S. Constitution requires state action, such is not the case under the California Constitution. That is why all employers should update their employee handbooks in light of the *Quon* decision.

Moreover, the rule of *Quon* is probably not limited to text messages. Employees' comments on Twitter, Facebook and all social media may be fair game. In essence, all communications — on whichever platform — may be fair game, if made using company equipment.

The moral of the story: companies should draft and implement clear, consistent and watertight usage policies — and regularly enforce their rights under such policies, without exception. The anxiety of both employer and employee may be soothed in knowing just where they stand.

If an employer supplies or subsidizes employees' computers or communications devices, company policy should clearly state that: Any messages employees send or receive on that equipment are subject to auditing by management; the examination of conversation transcripts may be reviewed if there are grounds to suggest misuse; and management need not use the least intrusive method of review. Further, employers would be wise before scrutinizing transcripts to disregard messages sent when the worker was off duty.

The updated usage policy will not only put employees on notice, but will protect employers from employee communications. For instance, where Employee A sexually harasses Employee B via a company computer, should the employer have known about it? If so, then the company is potentially liable for Employee A's misconduct. Or consider a less extreme example: Employee B complains that Employee A is harassing him. The employer should have a policy in place so that it can immediately investigate all of Employee A's communications on company systems.

For employees, the awareness that communications may not be private should always inform the content of those communications, i.e. to avoid posting steamy messages using company devices. For employers, consistently enforcing firm social media and technology policies will shield against costly litigation, and mitigate damages should a claim arise.

Eli M. Kantor and **Zachary M. Cantor** practice law in Beverly Hills. They represent employers and employees in all aspects of labor, employment and immigration law. They can be contacted at (310) 274-8216 or through www.beverlyhillsemploymentlaw.com and www.beverlyhillsimmigrationlaw.com.