

Social Media Policy — Still the Wild West

By [Melia Arnett-Archie](#) and [Jacey Kaps](#) | 2018-Sep-10



Executives at a Walmart woke up one morning in 2011 to a firestorm of attention. A store employee had posted to his Facebook page comments that were prompting outrage across the country. "We cater too much to the handicapped nowadays!" he posted.

"Hell, if you can't walk, why don't you stay the [expletive] home!!!!" He also ranted about poor people with large families, suggesting their population needed to be controlled just as deer herds are culled. His Facebook privacy settings were set to public, allowing anyone with a computer or smartphone to see his offensive posts, and, worse, that he was a Walmart employee.

In a world where remarks and images can spread on social media faster than a rampant wildfire, companies are finding that the greatest threat to maintaining the integrity of their digital reputation often is the indiscretion of their own employees. In addition to unleashing offensive opinions that may become associated with their employer, employees also are insiders who can blast damning criticism of their employers that may resonate in the marketplace.

All businesses — law firms and their clients — struggle with managing risk in this area where individual free speech rights clash with a business' rightful concerns about maintaining the integrity of its online reputation. Cultural norms, contentious political environments, speech and privacy laws, and the pervasiveness of technology and social media must all be considered when crafting policies that draw boundaries for employees and reduce the risk of reputational damage for their employers. While no company can prevent employees' occasional misbehavior on social media, they can set standards for acceptable behavior and sanction employees who violate those expectations.

Number one crisis rule — act

Customers and clients understand that companies can be victimized by the bad judgment of employees. But they do expect businesses to get out in front of reputational problems. When Starbucks faced a social media-fueled crisis prompted by the insensitive treatment of two African-American customers in one of its stores, it didn't waste time on a fact-finding committee. Within days, the company announced a sweeping plan to educate employees on race relations, even closing stores for a half day so employees could attend the program. The company's swift action sent the message that it wanted to do the right thing, and soon the incident faded from the news and social media.

[Related: How to Counsel in a Crisis]

Walmart also acted decisively, firing the employee who made the offensive posts and issuing a statement abhorring the comments. The National Labor Relations (NLRB) board upheld the firing and also took the opportunity to comment on permissible social media policies.

NLRA Section 7 offers expansive protection of speech

The operative point of the law for the NLRB is Section 7 of the National Labor Relations Act, which was created to protect employees' right to organize or participate in unions. This section of the law affects social media policies even when union organizing is not the issue. Social media policies conflict with Section 7 when they prohibit employees from criticizing the company, supervisors or working conditions. That settled interpretation of Section 7 applies to most comments on workplace conditions, which the NLRB reasons are protected speech since criticism of an employer is inherent in employees' right to organize. Thus, a social media policy that says an employee can't post anything that disparages the company likely will not pass NLRB scrutiny.

On the other hand, there is no protection for speech that has no connection to the NLRB's carveout for comments on workplace conditions or "mutual aid" of employees. Employers are within their right to ban social media that is obscene or malicious. In the United States, an employee has a right to espouse Nazi views under the protection of the First Amendment, and an employer has the right to part ways with such a person in employment-at-will states.

Of course, employment controversies often have overlapping issues, and it's better to avoid these situations through social media policies and, perhaps, counseling of employees. As with everything in employment law, what works in one state may not work next door. The takeaway: Employment law always is a minefield, but you can prohibit obnoxious speech that can't be construed as comments on the workplace.

“ Customers and clients understand that companies can be victimized by the bad judgment of employees. But they do expect businesses to get out in front of reputational problems.

Social media policies must be specific

Many companies write social media policies that are broad, perhaps reasoning that it is impossible to highlight every possible type of violation. A broad sweep of prohibitions or prescriptions would seem to give companies discretion in how they apply social media policies, but it also gives employees little firm guidance on what they can or cannot do.

The NLRB suggested in its discussion of the retailer's case that social media policies are more likely to survive review when they offer examples of prohibited behavior. "Be responsible" doesn't offer much guidance, but listing examples of prohibited behavior clarifies expectations for employees and makes it easier to support disciplinary action.

What you must prohibit

Any behavior you ban in the physical workplace should be banned on social media. As a baseline, this includes criminal behavior, dishonesty, and any activity that could have legal consequences (e.g., bullying, defamation, threats of violence, discrimination, and sexual harassment). Social media policies must not only prohibit such behavior, but also create mechanisms for targets of such posts to seek redress from the company. While it might seem unnecessary to ban illegal behavior, not all such posts will result in a criminal complaint. Requiring employees to acknowledge that such behavior is illegal and cause for the dismissal will make it easier to take disciplinary action.

[Related: 5 Considerations for an In-house Litigator When Guiding a Social Media Campaign]

Some prohibitions seem obvious but should be included in social media policies. That includes no expectation of privacy when using company computers or smartphones, and the misuse of proprietary information, intellectual property, and trade secrets. If a company is an industry with strict privacy legal standards, such as healthcare, social media policies should reflect those legal compliance standards.

Cyberbullying and sexual harassment directed from one employee to another might seem at first glance an issue that doesn't involve the company. However, even if the company is in no way complicit in the bullying or harassment, it may be seen as evidence of a hostile workplace. Once an employer becomes aware of such conduct, action must be taken. Cyberbullying, by the way, is now a crime in more than half of the states.

Monitoring is legal, but...

It's not illegal to look at employee social media feeds that are public, but it is nonetheless dangerous. The problem is that most social media accounts will reveal protected status information about employees (e.g., age, ethnicity, and disability). Employees who challenge dismissals or disciplinary actions can claim they were targeted because of information an employer saw on social media. This can be particularly problematic if you check out a prospective employee as part of a screening process. Don't go fishing in your employees' social media.

Some employers have taken an aggressive stance in monitoring workers, demanding as a condition of employment their social media account passwords or forcing them to accept managers as connections or friends. Unless the job involves national security, this is incredibly ill-advised and is banned in several states.

Europe is a different playing field

Companies work with EU companies will need social media policies specific to the European Union. While monitoring employees' social media is ill-advised in the United States, it is exceedingly treacherous in the European Union. Europeans have a conservative view of privacy rights, in stark contrast to the United States, where most people will trade their privacy for a free coupon. Europeans remember the efficient record keeping on individuals accomplished by the Third Reich and the horrifying consequences.

GDPR is complex but it has two overarching principles: consent and ownership. Employers must obtain consent for any data collection or monitoring of employees, and the individual owns his or her data and can demand, under certain circumstances, that it be destroyed or "forgotten." Essentially, social media policies that work in the United States likely will invite trouble in the European Union.

“ Cyberbullying and sexual harassment directed from one employee to another might seem at first glance an issue that doesn't involve the company. However, even if the company is in no way complicit in the bullying or harassment, it may be seen as evidence of a hostile workplace.

Do we have to allow an employee to say that?

Employers may believe they have a right to expect employees not to disparage them on social media. While common sense should tell you that criticizing your employer is not the best way to get a promotion, it may be protected speech, and employers must tread carefully in prohibitions.

In *NLRB v. Pier Sixty LLC*, a catering company employee went on his public Facebook page to call his supervisor a "nasty [expletive]." A Second Circuit panel, clearly troubled by the post, said it "sits at the outer bounds" of protected employee speech, but nonetheless sided with the employee. But context was everything. The company was in the middle of a tense standoff with workers who were about to vote on union certification, and the supervisor who was the target of the comments had provoked the Facebook comments by allegedly mistreating the employee. The court also pointed out that company supervisors used the same kind of salty language in their interactions with employees.

Be proactive in branding

Every company eventually will have to deal with the online indiscretions of a rogue employee. With such incidents in the news arising almost daily, the public understands that companies are caught off guard. In addition to acting quickly and publicly, companies are in a better position to withstand brand erosion when they have a long track record of stating their values in the marketplace and living up to them. Use your website and social media channels to tell your story and commitment to integrity. Let the public know the standards you set for your employees and promote the positive things you do in the community.

[Related: [How Legal Departments Can Help in a PR Crisis](#)]

The ubiquity of social media coupled with the current coarseness of discourse in our culture will only increase the incidents of individuals acting out on social media and the law will continue to evolve. But with constant reinforcement of your brand, you can send the message to customers and clients that individuals speak for themselves, not your business.

About the Authors

Melia Arnett-Archie is the senior privacy and data protection counsel at Stryker Corp., a global medical technology company based in Kalamazoo, Mich. From her office in the Miami-Fort Lauderdale area, she directs the company's global privacy strategy. She holds the CIPP/US accreditation from the International Association of Privacy Professionals.



Jacey Kaps is a partner in the Miami office of Rumberger Kirk & Caldwell, where he provides guidance on cybersecurity risks. He also holds the CIPP/US accreditation and the designation of Payment Card Industry Professional (PCIP) from the Payment Card Industry Security Standards Council.



The information in any resource collected in this virtual library should not be construed as legal advice or legal opinion on specific facts and should not be considered representative of the views of its authors, its sponsors, and/or ACC. These resources are not intended as a definitive statement on the subject addressed. Rather, they are intended to serve as a tool providing practical advice and references for the busy in-house practitioner and other readers.