Social Networking in the Retail World

Insights
9.01.10

Employer interest in social networking and blogging first came to the headlines when a flight attendant was fired purportedly for posting information about her job on a blog. Since that time, social media has exploded with the rise of Facebook and the advent of YouTube. While the Oxford English Dictionary has not yet recognized "tweet" as a verb meaning to post 140-character messages on Twitter, it must be coming.

The response of employers to their employees' use of these very public forms of communications has varied. Some employers actually encourage employees to blog about work. Others expressly prohibit it. Internet access to social networking sites has been terminated in many workplaces. Not deterred, employees have replaced the 90's bane of customer service, personal phone calls on cell phones, with texting and viewing prohibited websites on smart phones. Many people have experienced the frustration of being waited on by a clerk who is talking on a cell phone. That experience would be just as frustrating if the clerk were typing away on a mobile device.

But as the human resources side of retailers has struggled to eliminate these workplace distractions, the marketing side has gone the other direction. It is rare to find a retailer, from the largest in the world, to the most specialized one-person watch shop on a side street in small town USA, that does not have a Facebook fan site. Marketers are attempting to drive traffic to stores by tweeting specials to followers. Companies have their own YouTube channels. Some have created community forums for discussions on their websites. CEOs of major retailers have blogs featuring video appearances and opinions about their business. A customer's posting a negative comment about an experience can lead to the company sending out an apology letter with coupons for free or reduced-price items.

The specter this creates for many retailers is the dichotomy between providing wide public access and ability to comment, both good and bad, versus the desire to prevent destructive and harmful comments by disgruntled employees. Anyone with a Facebook account can comment on most Facebook fansites. Employees often make flattering and positive comments through this media. It is also not unusual to see individuals identifying themselves as employees countering negative comments that others have posted about their company.

The question then becomes what happens when the defense to a discrimination claim is "We fired an employee because we did not like what they said on our Facebook site even though it was true?"

Regardless of legality, a jury may well respond poorly to such an explanation since the company created the opportunity for the employee to publicly post comments.

This aggressive use of social media by retailers requires that you have policies for your employees that serve your business's interests without appearing draconian. The key to this approach is to align policies with the company's overall Internet presence while setting forth the prohibitions in the context of protecting your company against more than simple negative publicity.

Amending Existing Workplace Policies

Social networking at the place of business has become a tremendous drain on productivity for all types of businesses. According to a 2009 survey conducted by Deloitte LLP, 55% of employees visit social networking sites at least once a week and 20% admit to visiting social networking sites during work hours. The survey also states that 33% of employees do not consider the business implications of Internet postings.

Unlike the office setting, retail store employees are not as likely to have employer-provided Internet access. Instead, social networking activity will most often be carried out over smart phones and can easily violate general conduct rules already in place. Regardless of whether employees are writing on a blog, texting friends, or uploading pictures from a party, they are not doing their job. To eliminate these distractions, an employer can lawfully prohibit employees from having cell phones on their person while on duty. This not only prevents social networking, it also eliminates other distractions such as games, texting, web surfing, watching videos, and personal phone calls.

Where employees do have employer-provided Internet access, using those resources for social networking will often fall outside an employer's current acceptable use-of-technology policies, because the use is not business related. Particular conduct can also violate harassment policies, confidentiality policies, and security policies.

In most cases then, current policies already regulate undesirable conduct at the workplace. These can easily be updated to include social networking as an example of a situation where an employee's conduct could cross the line. A policy that prohibits employees from discussing information about customers could be updated to prohibit "posting information about customers online." It could also prohibit photographing customers, vendors, and co-workers as there are currently websites devoted solely to exhibiting pictures taken of individuals shopping at retailers. The key is to examine what is in place and amend those policies to make sure that they reference these new media as inappropriate.

Creating An Effective Social Networking Policy

Directly regulating an employee's off-duty social networking conduct is a much more complex proposition. First, social networking policies are not a one-size-fits-all proposition. For example, a computer retailer might want its employees to spend time on the Internet becoming familiar with and using the latest trends in this area. They may want their employees to be on forums discussing cutting edge computer issues. This would allow them to maintain a cutting edge image and educate cutting edge computer issues. This would allow them to maintain a cutting edge image and educate customers on the latest and greatest ways buying a computer could enhance their lives. A grocery retailer, on the other hand, has no such need.

To this end, the first aspect of designing a social networking policy is to examine how your company's employees' social networking activities can enhance or detract from the company's image. Do your employees' web presences enhance your company's reputation? How do your employees' activities fit with the company's Internet marketing strategies? What is the potential damage to your company's Internet presence by allowing employees to talk about their jobs in public forums? Will your instructions to employees impact your customers' image of your business, and if so, how?

Where employers see opportunities for the employees' activities to support and improve their brands, social networking policies will tend to be less restrictive. Where a company is highly sensitive to negative attention, these policies will likely be more restrictive. The key is to have a policy that fits the company's overall brand and Internet presence.

In either environment, there should be a set of rules designed to prevent common risks that should be included in a policy. First, the company should prohibit employees from using the name, trademarks, logos or copyright-protected material of the company or its clients. Employees should also be prohibited from making any statement that suggests any information that they post is either approved by or the official opinion of the company. You should also prohibit employees from listing their company email address unless the social networking site is used purely for company business or professional purposes. Even if the company's name is not used, the policy should prohibit posting anything obscene, vulgar, defamatory, threatening, discriminatory, harassing, abusive, hateful, or embarrassing to a fellow employee, vendor or customer.

There are other areas that companies will want to assess individually. The first is information the company desires to keep confidential. In the retail world, this will most often deal with pricing. An employee can easily negatively impact today's business by prematurely posting information about future pricing situations. Companies should assess the types of information they want to keep confidential and prohibit posting it as part of the policy.

And consider information about customers. In different situations, retail employees may have access to little customer information beyond perhaps a first name. But in others, the employees could have reviewed credit reports, loan applications, or buying histories. An employee posting any of this information could easily destroy valued relationships. Employees thus should be prohibited from posting any information about customers they obtain through their employment.

The Internet is rife with comments by purchasers on almost any product that can be bought. Many retailers allow for customer comments about products on their websites. Companies need to consider whether employees should be prohibited from commenting on products the company sells. Should an employee be allowed to post that a purchased item was shoddily made? Should employees be allowed to post, but only with restrictions that prevent any suggestion of relationship to the retailer?

At the end of the day, individual retailers need to determine how much or how little they want employees to participate in the online forums they have created.

A Word Of Caution

Cases revolving on employers terminating employees for engaging in social networking activity are in the early stages and many legal issues remain to be worked out. Be aware that some states prohibit terminating employees for lawful off-duty conduct. To what extent these statutes prohibit employers from terminating an employee for making a truthful but derogatory statement about his employer on a social networking site remains to be seen.

Likewise, employers should never access password-protected sites to which they have not been properly granted access, as doing so resulted in one national restaurant chain being found to have violated the Stored Communications Act of 1986. Finally, employees' conversations about working conditions on social networking sites may constitute concerted protected activity under the National Labor Relations Act. Thus, while it is appropriate and important that you have a policy to notify employees what behaviors you expect them to avoid, you need to carefully consider each individual situation before taking action based on a violation of the social networking policy.

Related People

Edward F. Harold
Regional Managing Partner
504.592.3801
Email