Portfolio Media. Inc. | 860 Broadway, 6th Floor | New York, NY 10003 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

Corporate Reputation Management Vs. Employee Privacy

Law360, New York (July 29, 2015, 12:39 PM ET) --

Kara Lyons

Social media has made corporate brand and reputation management more challenging, while at the same time fundamentally altering an employee's privacy profile. Information posted by or about an employee can have a deeply negative impact on a company's image, and the rapidity of its spread can be astounding. Companies are responding by more carefully monitoring employees, including employees' presence on social media.

The advent of "big data" allows companies to rapidly analyze large amounts of information and sift out the data relevant to its own employees, and gives employers even more tools to manage reputational risk through monitoring employee behavior. Common security technology allows companies to access personal information stored on company devices. The availability of this technology eases companies' ability to manage their brand and reputation. Where is the desire and responsibility to manage company reputation limited by an employee's right to privacy?

Consider the following hypothetical situations:

1) A company executive entertains potential customers at a strip club. After having a few too many cocktails, the executive's behavior gets increasingly out of control. Eventually, the executive is asked to leave the club. After refusing, he is forcibly removed from the establishment by local police. Much of the evening is captured on social media, with witnesses posting pictures on Facebook, tagging the executive and including negative comments regarding the company. Other witnesses tweet about the executive's behavior, and the tweets are rapidly retweeted. One witness records the executive's forcible removal from the club with his smartphone and posts the entire episode on YouTube. Overnight the video receives several thousand views. Through regular monitoring of social media postings about the company and its employees, the company learns of these events by the next morning. The company terminates the executive's employment the next day as a result of the executive's behavior, and commences public relations efforts to mitigate the damage to its reputation.

2) Most nights after work, a company executive stops at a liquor store, purchasing a fifth of scotch, and then at an adult video store, renting pornographic movies. This behavior is unknown to the employer and has not had a visible impact on his performance. A new data analytics system accessed by the

company allows it to analyze large amounts of information about their executives, in order to spot trends that might lead to behavior potentially damaging to the company. When combining scans of credit card data with the GPS tracking features in the executive's company-issued smartphone, the company learns of the executive's regular after-work pattern. The company confronts the executive about his behavior, and he admits to consuming several fifths of scotch each week, and spending hundreds of dollars on pornography and at strip clubs. The company further confiscates the executive's company-issued smartphone, on which he has installed a personal email account. Using common password-breaking technology, the company is able to access the personal email account and confirm that he has used the smartphone to register for online pornography. The company terminates the executive's employment based on the executive's unseemly behavior, which it fears will have a negative impact on the company's reputation.

Employers use social media both to monitor employee behavior damaging to the company and to monitor employee communications relevant to the employer. Currently, both state and federal law allow employers broad authority to monitor employees provided the monitoring is done for a legitimate business purpose. Employers can access information posted online by third parties, use GPS or other technology to track employees while on the job, and, in most circumstances, monitor employee social media activity on company computers and devices. This authority, though, is not without limits and risks.

Statutory Employee Privacy Protections

Although no U.S. or state law specifically addresses employee privacy in the workplace, certain laws and causes of actions intended for other purposes have been used by courts and administrative bodies to evaluate certain aspects of employee privacy. For example, several federal statues, which were originally intended to prevent such activities as wiretapping or hacking of computer systems, have been applied to restrict employer access to employee social media. Among others, the Electronic Communications Privacy Act (ECPA), the Stored Communications Act, and the Computer Fraud and Abuse Act all serve as hurdles for an employer seeking to view the social media activity of its employees.

The ECPA protects the privacy of employee communications. In the employment context, claims under the ECPA have not been widely successful because the law provides a specific exception for interception of communications when the company has a legitimate business interest in monitoring the communications. The Stored Communications Act prohibits an employer from intentionally obtaining, altering, or preventing authorized access to certain stored communications. At least one court has found that an employer violated the Stored Communications Act by firing employees for comments posted on a password-protected MySpace page after the employer obtained, though the apparent coercion of one employee, the login and password information for the MySpace page.

Certain states explicitly recognize an individual right to privacy in state constitutions or statutes. Even those states without constitutional or statutory rights to privacy recognize the common law tort of invasion of privacy. Generally speaking, a constitutional, statutory or common law right to privacy prevents employers from unreasonably intruding into the "seclusion" of their employees. The determination of whether an employer's monitoring of an employee's social media violates the employee's privacy will often turn on whether the employee has a reasonable expectation of privacy.

In the employment context, an employee's right to privacy is generally diminished. However, employees may still have an expectation of privacy when using company equipment to send private communications. For example, one court has prohibited an employer from accessing its employee's

emails sent to her attorney using a Web-based, password-protected email service (e.g., Gmail or Yahoo!), despite a company policy expressly informing the employee of employer monitoring, and despite the fact that the activities took place on facilities and equipment provided by the employer. Other courts have found that an employee has no expectation of privacy when using a company-provided computer to communicate via email or social media.

Additionally, state laws generally intended to protect off-duty activities may also protect the privacy of employees in digital world. Several states, including Colorado, have statutes prohibiting employers from taking any job-related action against an employee based on that employee's lawful conduct off the job. If, for example, an employer finds photos on social media of an employee consuming alcohol, so long as the employee is of legal drinking age, the employer may not terminate that employee for such behavior under these types of laws, even if the employee's behavior reflects negatively on the company.

Finally, despite the absence of general workplace privacy laws, certain states have passed laws precluding employers from asking employees or applicants for employment to disclose social media passwords or requiring employees or applicants to allow an employer access to nonpublic information posted through social media.

Other Enforcement of Employee Privacy Rights

Federal and state agencies tasked with protecting employee rights have taken note of employee privacy issues in today's digital age. In particular, the National Labor Relations Board has issued guidance and several decisions seeking to protect employee's actions on social media under the National Labor Relations Act. The NLRA prohibits an employer, whether unionized or not, from interfering with employees who come together to discuss or address a collective employee concern. The NLRB is tasked with enforcing the protections of the NLRA, including regulating employer policies that may prevent employees from engaging in this type of concerted activity in both unionized and non-unionized workplaces. Relying on the NLRA, the NLRB has recently issued guidance regarding employee's right to use social media and several opinions invaliding employer social media or other employment policies for stifling employees' right to engage in this type of "concerted activity."

For example, the NLRB recently found that an employer violated the NLRA when it terminated two employees for participating in a Facebook discussion criticizing the employer's failure to withhold the proper amount of state income tax from their paychecks. The NLRB deemed the employer's social networking policy — which threatened employees with discipline for publicly sharing information "related to the company or any of its employees or customers" — unreasonably broad and vague under the NRLA. The NLRB concluded that the language in the policy could restrain the employees in their right to freely communicate with their fellow employees regarding work issues. The NLRB also determined that an employer violated the NLRA by firing an employee for defying an "insubordination rule" set forth in the company's handbook after the employee posted disparaging comments about coworkers and managers on social media. In each of these cases, the employer's policy was deemed invalid because the policies were not clear enough to ensure employees were permitted to engage in conduct specifically protected under the NLRA.

Employers are further limited by laws prohibiting discrimination and retaliation against employees.

A Delicate Balance

There are substantial limits and risks when an employer monitors and acts on the basis of employee

activity on social media. Those limits are defined by various laws and, in some cases, by the employee's fundamental right to privacy.

In analyzing the two hypotheticals presented above, an employer would likely be justified in terminating the strip club bruiser in the first example. Not only was the incident public (unlike a private Facebook post between friends), but the executive was also acting in a disruptive and unlawful manner and, at the time of the incident, was acting within the scope of his employment duties on behalf of the company. If the same scenario involved an employee who posted drunken pictures to his private Facebook wall while off duty, the legal analysis of his termination would certainly change.

The second hypothetical moves us into these deeper privacy rights. The employee terminated for his off-duty conduct would have much stronger grounds on which to bring claims against his employer. Not only are his off-duty activities legal, but absent any company policy or handbook notifying the employee of the employer's use of monitoring technology, the employee may be able to establish he had a reasonable expectation of privacy as to his personal activities on the smartphone. The employer's monitoring of the employee's off-duty conduct could result in a cause of action for invasion of privacy or other related claims.

Employers must consider the various legal issues at play in light of the technology-related issues now confronting employer reputation management and employee privacy. Employers should implement social media and electronic communications policies that are drafted carefully and clearly. In particular, the policies should avoid generalities which appear to limit employee's rights, such as prohibiting employees from "disparaging" the company in anyway. Instead, the policies should include specifics, such as prohibiting the employee from using language in electronic communications that is vulgar, obscene, threatening, intimidating, harassing, or in violation of the employer's anti-discrimination and anti-harassment policy. Social media and electronic communications policies should also include an explicit disclaimer, explaining that the policies do not prohibit the employees from engaging in the concerted activity protected by the NLRA.

Employers should also establish procedures and guidelines for conducting employee monitoring. Employers should apply these guidelines consistently for all employees to avoid allegations of discrimination. When monitoring employees online, employers should only access information available to the public, and should not require or request employee passwords to access additional information. Employers opting to use new technology to monitor individual and group wide behavior outside of the workplace should be strictly regulated. Employers should exercise extreme caution if monitoring the behavior of employees off-duty to avoid running afoul of any lawful conduct protections of the employee. Additionally, employer policies should explicitly state when the employer may access employee devices, such as smartphones and laptops for the purpose of monitoring. If employers are aware employees are using company-issued devices for personal purposes, employers should consider whether encouraging employees to use secure services for personal email and text is appropriate given the role of the employees and the potential risks of employee privacy violations.

—By Rob Kilgore, Absio Corporation, and Kara Lyons and Nicole Truso, Faegre Baker Daniels LLP

Rob Kilgore is the president and CEO of Absio Corporation and a former Colorado lawyer.

Kara Lyons is an associate in Faegre Baker Daniels' Denver office.

Nicole Truso is an associate in the firm's Minneapolis office.

The opinions expressed are those of the author(s) and do not necessarily reflect the views of the firm, its clients, or Portfolio Media Inc., or any of its or their respective affiliates. This article is for general information purposes and is not intended to be and should not be taken as legal advice.
