News & Publications

Do’s and Don’t’s of Monitoring the Activities of Employees on Social Networking Sites

Author: Lisa I. Fried-Grodin

New Jersey Law Journal

December 6, 2010

With the ever-growing popularity of social networking sites, and with so many employees exercising poor judgment online, it's easy to understand why employers are concerned about the messages and images that that their employees are disseminating on these websites.

For employers, the costs are real: Poor choices by their employees can bring with it not only bad publicity but the loss of confidential information and the risk that the employer and employee will be sued by a third party for a wide range of legal claims, including defamation, invasion of privacy, negligence, discrimination, false light publicity, public disclosure of private facts, infliction of emotional distress and violations of state and federal data breach laws.

Employees seem to comprehend the potential effect of their online rants. According to the 2009 Deloitte Ethics and Workplace Survey, 74 percent of employees believe it is easy to damage a company's reputation on social media sites. Yet, many conduct themselves as if they have a right to do so. Fifty three percent of the employees surveyed believe that an employee's social networking page is not

their employer's business, and nearly one-third said they never consider what their boss would think before posting material online.

Social media content is also becoming a new source of evidence in employment cases. Employers view such material as a unique way to identify false statements employees make in these cases. Employees, however, often view their employer's interest in such content as an invasion of their privacy.

These divergent viewpoints are creating new tensions in the workplace and new issues for the courts to address. A look at some of the cases that are emerging sheds some light on the issues facing employers and employment lawyers in this new technological era.

Did Conduct Occur on Company Computers?

The decisions that a company makes regarding whether or not to block employees from using social networking sites at work can affect the liability the company faces for conduct flowing from employees' online conduct. In *Yath v. Fairview Clinics*, 767 N.W. 2d 34 (Minn. App. 2009), a patient sued the Fairview Cedar Ridge Clinic, two employees and others for several legal claims, including invasion of privacy, after learning that clinic employees had reviewed her medical file, learned that she had a sexually transmitted disease, disclosed this information to other people, and the information showed up on MySpace.

The clinic had previously blocked employees from accessing MySpace at work, and that decision helped the clinic win summary judgment when the patient sued the clinic for invasion of privacy. The trial court held, and the appellate court affirmed, that because MySpace was blocked at the clinic when the patient's information appeared on it, the content at issue could not have been created at the clinic. Because it was unclear who posted the MySpace content, the trial court also dismissed the invasion of privacy claim against the employees.

On the other hand, when an employee posts inappropriate material on social networking sites using the employer's computer, such a defense disappears. Indeed in those instances, liability for the employer can turn on the steps the employer took to address the conduct.

For example, in *Delfino v. Agilent Technologies, Inc.,* 145 Cal. App. 4th 790 (Ct. of Appeal of Calif., 6th App. District 2006), cert. denied, 522 U.S. 817 (2007), Agilent was sued for intentional infliction of emotional distress and negligence as a result of cyber threats an employee

posted on Internet bulletin boards using Agilent's computer system. Agilent learned of the situation from the FBI, and once it confirmed it, it immediately terminated the employee. Because Agilent was not aware of the conduct when it occurred, the dissemination of the messages was not related to the employee's job duties, and the company swiftly terminated the employee upon learning of the situation, the court held that the company was not directly or vicariously liable for the tort claims.

New Jersey-based XYZ Corp. was not as fortunate. In *Doe v. XYZ Corp.,* 382 N.J. Super. 122 (App. Div. 2005), the wife of an employee of XYZ Corp. sued the company for negligence arising from the employees' use of XYZ's computers to post naked photographs of his stepdaughter on pornographic websites. The company was not aware that the employee had sent the photographs but was aware that he had visited several porn sites, including one that spoke about children. A supervisor told the employee to stop accessing such sites at work, but when that same supervisor later saw the employee doing it again, he did nothing about it.

In denying XYZ summary judgment, the court reasoned that the company could have done more to prevent harm to third parties, such as viewing the content on the websites the employee had accessed, reporting the activity to the police, and taking additional action to stop the conduct beyond warning the employee.

Another thorny issue facing employers is employee use of passwo rd-protected websites to bash their employers . Some employers who have learned of such sites and accessed them without permission have wound up in court, accused of violating the Stored Communications Act. ("SCA") 18 U.S.C. §2701 et seq. The SCA makes it unlawful to intentionally access a stored electronic communication without authorization.

In *Pietrylo v. Hillstone Restaurant Group*, 29 IER Cases 1438 (D.N.J. 2009), for example, two employees of Houston's Hackensack, N.J., restaurant set up an invitation-only MySpace chat group "to vent about any BS we deal with [at] work without any outside eyes spying in on us." Posts on the site included sexual remarks about management and customers, jokes about Houston's customer service, references to violence and drug use, and a copy of a new test that was to be given to employees. An employee accessed the site and showed it to a manager. This prompted the company to request the password from the employee and log onto the site five times to view its contents. After Houston's terminated the two employees who started the site,

the two employees sued the company that owns Houston's for violating the SCA. The jury found for the employees and awarded them lost wages and punitive damages.

New Source of Evidence

With so many employee posting private information about themselves on social networking sites, the content on these sites is providing new evidence in employment cases. For example, in cases involving a disability discrimination claim or a claim for emotional distress damages, the employee's social networking site content can provide relevant evidence regarding the legitimacy of the employee's alleged medical conditions and injuries.

That's what Simply Storage argued in *EEOC v. Simply Storage Management, LLC*, (U.S. District Ct. So. District of Indiana, 2010), a case involving claims by two women that they were was sexually harassed at work and suffered severe emotional distress. Simply Storage issued discovery requests for photographs or videos posted by the plaintiffs or anyone on their behalf on their Facebook or MySpace pages, electronic copies of their Facebook and MySpace profiles, status updates, messages, wall comments, groups joined, activity streams, blogs and comments during the period of the alleged emotional distress.

The EEOC responded that that the requests infringed on the women's privacy and would embarrass them. The court held that a person's emotional distress can manifest itself in social networking site content and ordered the production of the material requested to the extent that it regarded any emotion, feeling or mental state.

Employers are also starting to use employees' LinkedIn contacts and Facebook friends as evidence in cases involving breach of a noncompete or nonsolicitation agreement. In March, Maryland-based TEKsystems, Inc., an information technology search firm, sued three former employees for breaching noncompetition and nonsolicitation agreements and for other claims. *TEKsystems, Inc. v. Hammernick*, Case No. 10-CV-00819 (U.S. Dist. Ct. Minn. 2010). In support of its claim that one former employee breached a non-solicitation agreement restricting her from soliciting TEKsystems employees, TEKsystems alleged in the complaint that the former employee sent messages to at least 20 of its employees on LinkedIn to assess if they were still looking for other career opportunities. The case settled in October.

On the flip side, thanks to the amount of information available on social networking sites, employees who are not subject to post-employment restrictive covenants have a new way to challenge the confidentiality of their employer's customer lists. See, for example, *Sasqua Group, Inc. v. Lori Courtney*, 2010 WL 3702468 (Eastern Dist. Of N.Y. 2010).

Preparing for the Future

As hardly a month goes by without a news report that an employee was fired over their Facebook posts, new issues will continue to emerge for employers. Those that re-examine and modify their policies, employment agreements and practices to account for employee use of social media will be the best prepared to address these issues when they arise.

Fried-Grodin is an associate in Fox Rothschild's labor and employment group in Roseland.