EMPLOYEE PRIVACY IN THE AGE OF WORKPLACE MONITORING

Kristin M. Case
The Case Law Firm, LLC
250 S. Wacker Drive, Suite 230
Chicago, IL 60606
312-920-0400
http://www.thecaselawfirm.com
http://www.blog.thecaselawfirm.com
I. HOW EMPLOYERS “MONITOR”

a. Pre-Employment “Screening:”

i. Beware: A June 2009 CareerBuilder survey of more than 2,600 managers found that 45% of employers reported using social networking sites to research job candidates and another 11% said that they planned to start doing so.

1. Employers can use this publicly available information to weed out protected classes, such as minorities, parents, applicants of certain ages or sexual orientation and/or individuals with health conditions or disabilities. Now of course this is not legal but the difficulty in proving the discriminatory use of social media in a hiring decision makes a nearly impossible failure to hire claim even more difficult.

2. Employers may also use these social media sites to weed out employees who may be taking part in unlawful activities—such as drug use. Think of the employee who posts a picture of himself smoking pot with his buddies on the weekend.

ii. Background Checks:

1. The ones you know about: This occurs when an employee signs a release authorizing an employer to conduct a background check.

2. The ones you do not know about: informal Google and other Internet searches.

iii. What about the Fair Credit Reporting Act?: The federal Fair Credit Reporting Act (FCRA) sets national standards for employment screening. However, the law only applies to background checks performed by an outside company, called a "consumer reporting agency." The law does not yet apply in situations where a manager or HR representative informally Googles an applicant’s name. Thus, social media sites allow employers to circumvent the protections afforded by the FCRA which require an outside agency to have the employee’s consent prior to conducting a background search.
1. Note, however, that if the employer retains an outside agency to conduct the background search and part of that background search involves an online investigation then consent would be required. The key here is whether a third party has been retained or whether a hiring manager is simply doing this himself.

b. Monitoring Workday Behavior:

i. **Beware:** According to a 2008 study by the American Management Association, 66% of employers monitor Internet connections, and 45% engage in various forms of computer monitoring such as email scanning, video surveillance, tracking content, keystrokes, time spent at the keyboard and location/GPS monitoring.

   1. If an employee is doing something on an employer’s computer then the employer may monitor it.

ii. **Video Monitoring:** In order for an employer to legally videotape an employee it must have some legitimate business purpose - but this is not hard to meet. According to a 2001 study by the American Management Association, more than 15% of midsize and large companies used video surveillance to monitor employee job performance, and almost 38% filmed employees for security.

   1. Federal law does not prohibit video monitoring although some states do.

   2. Note: Some states, including Illinois, maintain strict two-party consent laws regarding audio recordings. In those states, even where video surveillance is supported by a legitimate business purpose, the recordings cannot record audio without employee consent.

iii. **Location Monitoring:** This is the current hot button issue in employee privacy.

   1. GPS: Only California has enacted a law that prohibits a private employer from tracking an employee’s personal vehicle. Employees in the other 49 states must rely on invasion of privacy arguments.

   2. Smartphones: Smartphones, generally, track the location of their users. Thus, employees who use company issued smartphones are
giving their employers the right and the ability to track their whereabouts; not just during the workday but after-hours as well.

3. In Cunningham v. New York Department of Labor, 933 N.Y.S.2d 432 (N.Y. App. 3d Dept. 2011) the Appellate court found that the public employer’s use of a secretly planted GPS monitoring device on an employee’s public vehicle was reasonable and did not amount to an illegal search. While this case dealt with certain constitutional rights, this is instructive as to what courts would decide with respect to a private employer.

4. Compare with: U.S. v. Maynard, 615 F.3d 544 (D.C. Cir. 2010), a decision by the federal court of appeals in the District of Columbia which suggests that, in certain circumstances, employers who track their employees’ location could face liability for invasion of privacy. In this case the court held that the FBI had infringed upon the criminal defendant's reasonable expectation of privacy by “tracking his movements 24 hours a day for four weeks with a GPS device they had installed on his Jeep without a valid warrant.”

c. Monitoring Leaves of Absence:

   i. **Beware**: Employers can and do continue to monitor their employees while they are on leaves of absence.

   ii. **Social Media Monitoring**:

      1. Consider a recent matter that just occurred in one of our cases: one of our clients had been receiving disability benefits for severe and disabling depression. Both she and her doctor continued to certify that her depression prohibited her from being able to work and that it limited her in many major life activities. After providing her with more than one year of disability benefits, the provider discontinued the benefits, citing postings on her Facebook page in which she talked about all the activities and charities in which she was participating. These public postings tipped off the disability provider who then enlisted video surveillance to determine that she was, indeed, taking part in many activities.

   iii. **Location Tracking**: See above.

   d. **Monitoring After Hours Conduct**: This is the area in which employees are provided the greatest protections.
i. **Social Media:**

1. First, a word of advice: Even if a social media profile is set to “private” a lot may be gleaned from the little bit that cannot be made private. For instance, MySpace allows the user to select a privacy setting, but the Profile “Headline” and profile picture can still be seen upon executing a name search. Similarly, with the implementation of new privacy settings on Facebook, many users remain confused about what information they can be seen by other users – whether they be friends, friends of friends, or people in similar broad networks such as “Chicago attorneys,” or various alumnae groups.

2. Ex: A small business to whom I provide employee-relations advice hired a new salesperson. The manager, out of curiosity, Googled her name and found that she had a MySpace page. The Page was set to private, however, her profile picture was of her in a very revealing bra in a very suggestive position. While the offer of employment had already been made the manager began the employment relationship with serious doubts about the employee and how customers might view the employer if they saw this picture.

ii. **Use of Company Cell Phone for Texts and Calls:** See above.

iii. **Location Tracking:** See above.

**II. EMPLOYEE PROTECTIONS**

a. **First Amendment:** Public employees may enjoy some First and Fourth Amendment protections depending upon the contents of a social media post or the intrusiveness of a “search” into their activities.

i. **Note:** First and Fourth Amendment protections only extend to public employees and, thus, private employees have no right to free speech in the workplace. It is important to advise your clients of this because the vast majority of employees tend to believe that the right to free speech travels with them to private employers.

b. **Federal or State Anti-Discrimination or Retaliation Statutes:** The content of the communication may offer its own protection. If the communication or posting that offends the employer is, for instance, of a religious nature, involves efforts to unionize, or pertains to certain gender or minority-based groups or adverse actions taken as a result of inclusion in such a group, the communication itself could form the basis of either a discrimination or retaliation claim.
c. **The Electronic Communications Privacy Act ("ECPA"):** The ECPA prohibits the interception of wire, oral or electronic communication without consent, but does not generally apply to an employer’s monitoring of its own e-mail or phone systems.

d. **The Stored Communications Act, 18 U.S.C. 2701:**

i. Enacted to ensure the confidentiality of electronic communications.

ii. Section 2701 states that an offense is committed by anyone who: “(1) intentionally accesses without authorization a facility through which an electronic communication service is provided;” or “(2) intentionally exceeds an authorization to access that facility; and thereby obtains...[an] electronic communication while it is in electronic storage in such system.” 18 U.S.C. § 2701(a)(1)-(2).

iii. Section 2511 makes it clear that this prohibition generally does not apply to an "electronic communication [that] is readily accessible to the general public." So, in the case of social media, the inquiry must turn on how the employer gained access to an employee’s posts. If the information was gleaned, for instance, from a Google search then the Act has not been violated.

iv. In *Pietrylo v. Hillstone Restaurant Group*, 2009 WL 3128420 at *1 (D. N.J. 2009) a federal district court upheld a jury’s verdict in favor of the plaintiff, including punitive damages, finding that the employer had violated the Stored Communications Act when two of its managers accessed a "chat group" on an employee's MySpace account without having received authorization from the MySpace member to join the group and, instead, by coercing another employee to give them her password. *Id.* at *1.

1. The lesson here? If an employee makes efforts to protect the social media information as private and an employer gets to that information in any other way aside from having the employee’s specific consent, liability could attach.

e. **Personnel Record Acts:**

i. Many states have enacted statutes which provide employees with rights regarding how an employer may gather, store and/or utilize “personnel” data.

1. *Ex: Illinois Personnel Record Review Act, 820 ILCS 40*
2. Sec. 9 states “An employer shall not gather or keep a record of an employee’s associations, political activities, publications, communications or nonemployment activities, unless the employee submits the information in writing or authorizes the employer in writing to keep or gather the information.”

3. The prohibition does not, however, apply to activities that occur on the employer's premises or during the employee's working hours.

4. The section also does not apply to those activities “which interfere with the performance of the employee's duties or the duties of other employees or activities, regardless of when and where occurring, which constitute criminal conduct or may reasonably be expected to harm the employer's property, operations or business, or could by the employee's action cause the employer financial liability.”
   
a. I suspect that employers will try to argue reputational harm under the italicized portion of the exception above.

f. Workplace Privacy Statutes:

   i. A number of states recognize private employees’ rights to some degree of privacy in the workplace, although these laws differ quite a bit from one another. They include: Alabama, Alaska, Arkansas, California, Florida, Hawaii, Illinois, Iowa, Louisiana, Maine, Maryland, Massachusetts, Michigan, Mississippi, Montana, Nebraska, Nevada, New Hampshire, North Carolina, Ohio, Rhode Island, South Carolina, Tennessee, Texas, Vermont and Wisconsin.

   ii. In California, Connecticut, Delaware, Michigan and Rhode Island, employers’ electronic monitoring of employees at work is subject to regulation, and prohibited in some locations within the workplace associated with a higher expectation of privacy, such as bathrooms. In Connecticut, for example, employers must give prior notice to employees of electronic monitoring in the workplace, absent reasonable grounds to suspect illegal conduct, a hostile work environment or other misconduct.

   iii. Ex: In Illinois, 820 ILCS 55 prohibits discrimination for use of lawful products outside of the workplace.

1. Section 5 states, “it shall be unlawful for an employer to refuse to hire or to discharge any individual, or otherwise disadvantage any individual, with respect to compensation, terms, conditions or privileges of employment because the individual uses lawful
products off the premises of the employer during nonworking hours.”

2. This Act was originally created to protect employees who faced termination for being smokers or drinkers. While social media was not even remotely on the radar at the time this Act was enacted, the language would certainly seem to prohibit taking an adverse action against an employee who lawfully uses social media off premises.

g. **Common Law Privacy Claims:**

i. [Restatement (Second) of Torts 652B (1977): Intrusion upon seclusion](#) is the type of invasion of privacy claim that could provide an employee with the best chance of protection because it is associated with either a physical intrusion into a place in which the plaintiff has secluded herself or a non-tangible intrusion into the plaintiff’s private matters. The claims that seem to be the most successful are those that entail either an extremely private matter or monitoring of employees outside of work.