# Big Brother

## When and How to Spy On Your Employees

By Jack Garson

***October 2010 – As seen in the SmartCEO Magazine.***

You just got back from lunch at your favorite restaurant, but you're sick to your stomach. While you were there, you saw your star saleswoman dining with your biggest competitor and there is no good reason on Earth for that to be happening. Now that you think about it, lately, your super-saleswoman has had her office door uncharacteristically shut, and when you've passed her in the hall, she has hardly looked you in the eye. There are a lot of questions racing through your mind. Is she leaving your company? Is she taking customer lists and other critical data with her? Can you look at her emails and other computer records to find out?

The advent of the computer age has spawned all kinds of benefits and problems. Information that took days, if not weeks, to travel from point A to B now flies over fiber optic lines at the speed of light. Contracts are negotiated via email and signed electronically. But on the other hand, just by hitting a send button, any one of your employees can do incredible damage to your company. And that's not all. Aside from shipping away your trade secrets, they could send harassing emails to co-workers, access porn sites, illegally download software or just waste time not working.

### Monitoring Policies

Subject to some very important caveats, you can monitor emails sent and received by your employees on company equipment. First and foremost, though, you need a very well written company policy that informs all of your employees that you reserve the right to see these emails. When courts have determined that monitoring is allowed, judges have focused on whether companies made it clear that their employees should not expect their emails to be considered private. So one of the key components of an effective monitoring policy is unambiguously stating that company computers and other equipment should not be used for personal communications and that you may and will read emails and other information as the company determines appropriate.

But there is a lot more to it than just that. Heed the following precautions as well:

- Make sure to spell out the fact that all company equipment and systems are subject to monitoring. Include all of the specific equipment, such as computers, cell phones, and pagers, which you are presently using. Then include a catch-all for items not specifically identified and for equipment that you might use in the future. There is a need for clarity and precision this can't be a slapdash string of words. Still, you can't think of everything, so make sure to include that broad catch-all language.

- You should also include certain prohibitions, such as strict rules against stealing company property, disclosing company secrets and other information, engaging in other inappropriate behavior, such accessing pornographic websites or sending obscene or defamatory communications.

- State that information produced on this equipment and systems is company property.

- Reserve the right to access and monitor usage, with or without notice. But be aware that some state or local laws may require that you notify employees when monitoring their electronic communications.

- Make sure to issue this monitoring policy to all of your employees, and if you update the policy, clarify which policy is in effect. Theoretically, it is great if you can get your employees to sign a receipt acknowledging that they received the policy and will comply. But this is tricky. You'll need to get that receipt from every employee, and we all know how difficult it is to implement this 100 percent of the time.

- Don't undermine your own policy. That is, don't adopt the policy and then tell people not to worry about it. In fact, your policy should provide that no one can create any exceptions to the policy except with the written authorization of certain specified officers of the company.

**Left -field Zingers**

The personal sensibilities of some judges seem to affect whether a company is allowed to monitor employee emails and the like. Where employees have been looking at porn or stealing from the company, then reading their emails despite an imperfect monitoring policy often receives the judge's hearty endorsement. But when an employee is engaged in truly personal communications, the court is much more likely to slap the company on the wrist or worse. In fact, once you realize how many judges disagree with each other, you'll understand that email monitoring can be a minefield. So watch out for the following IEDs.

- The Limited Personal Use exception. This one truly proves that no good deed goes unpunished. When companies have bowed to the reality that their employees will be using email for personal use hopefully limited and reasonable they have written their policies to include a limited personal use exception. Unfortunately, this exception can create a loophole that undermines the whole policy. So whatever you do, don't try to create a monitoring policy on your own. This is one of those tasks where you especially need knowledgeable legal guidance.

- Company computers in home offices. With the rise of telecommuting, more employees are working from home. However, some courts are reluctant to extend the reach of a monitoring policy into people's houses, even when company computers are used. If you want your monitoring policy to cover these computers and there are plenty of good reasons you should then do so expressly.

- The rules aren't always the rules. No matter what your policy says, some courts will make exceptions. In one case, the court said that even an iron-clad policy would not allow an employer to see employee's personal emails sent on company equipment.

- The hometown roast. Watch out for local laws. For example, California is particularly pro-employee and prohibits things that are commonly permitted elsewhere.

But if do you everything right, not only can you stop your super-salesperson from delivering the company jewels to the enemy, you may even prevent her from taking your clients and working for a reasonable time period for the competition. A good CEO hopes for and tries to inspire the best but still plans for the worst.

Jack Garson is the founder and a principal of the law firm Garson Law LLC in Bethesda, MD, and is also the author of "How to Build a Business and Sell It for Millions."

Jack Garson
Garson Law LLC
(301) 280-2700
jgarson@garsonlaw.com