Someone Controlling Your Cell Phone? Absurd! Or is it. . .

Insights
7.01.09

(Labor Letter, July 2009)

As if employers didn't have enough to worry about already, here comes the next big thing to fear:

- others can tap and listen in on your cell phone calls;
- they can know your exact location at any time your phone is on; and
- they can access the speakerphone on your cell phone and listen to you when you are not even on the phone.

A disgruntled employee need only type "How to tap a cell phone" into a computer's search engine to see the numerous results and the programs available on the market to illegally tap cell phones. It's no secret either – an Indianapolis news station recently ran a story about phone tapping and the downloadable software that can be installed onto a cell phone, resulting in a dramatic loss of privacy for the user.

The software is fairly inexpensive, easy to purchase online, and takes only ten minutes to download onto a phone. One website selling the software, www.flexispy.com, boasts that you can "Catch cheating spouses!" "Check on babysitters!" and "Bug meeting rooms!" The issues of illegality and serious invasion of privacy may not overly concern a malevolent outsider or an embittered employee.

A Primer On Privacy
Here's how it works. Just give the "tapper" 10 minutes alone with your cell phone and voila! The tapper can read your text messages, activate the speakerphone when you are not even on the phone and listen to your live conversations, track your movements, and see your call log of incoming and outgoing calls. In fact, when you are receiving a call, some programs will text the tapper so they can call in and listen to the conversation.

Of course such programs are highly illegal and can carry jail time but this is no consolation if you lose valuable company secrets or personal information leaks out to employees or third parties. You may remember just a couple of years ago when a similar problem with Bluetooth headsets arose. Hackers were able to hack into the headset, have it connect to their laptop or cell phone, and then hear the conversations taking place. This new technology is similar but evem more extensive in its reach.

Assessing The Risks

Although not meant to unnecessarily alarm you, here are a few ways this type of cell phone tapping can affect you and your company. Disgruntled employees can listen in to what you are saying about them or other employees, creating a serious effect on workplace morale and efficiency. Such information has a way of spreading quickly, leaving you to put out fires you did not even know you had started.

Additionally, labor unions may use this technology as an organizing tactic to figure out what you are telling your employees, and to undermine you. Knowing the ins and outs of your business, they can use such information to their advantage.

A final example regards competitors. Using this technology, competitors can easily obtain your confidential information about employees, or trade secrets including operating mechanisms, account numbers, and similar information.

Protecting Yourself

In addition to keeping your employees happy (and so less likely to want to harm your company), and having enforceable confidentiality agreements, here are a few more tips to protect yourself:

- turn your phone off when it is not in use and remove the battery;
- try to conduct conversations with co-workers in person, as opposed to calling them up on your cell phone;
- never leave your phone unattended;
- put a password on your cell phone so even if someone gets a hold of it, he or she cannot upload the software;
- set your Bluetooth headset to not accept anonymous requests and also put a password on it so it cannot be accessed by others; and
- check into anti-spy software that will protect your phone.

After making sure you are protecting the actual cell phone you are using and making sure all management personnel are aware of the risks of leaving their phones unattended, make sure you have valid and enforceable confidentiality agreements and non-compete agreements in states where these are allowed. Making sure your information is protected if it leaks out will leave you with some recourse if an employee happens to follow the highly illegal route of tapping your cell phone and stealing your confidential information.

In addition, make sure your employee handbook and policies disallow personal cell phone usage during work time. And try to limit phone usage to land lines whenever possible. It's better to take precautions now than to attempt to recover confidential materials or fight a disgruntled employee later.

A version of this article was reprinted in the July 6, 2009 issue of *Employment Law360*.